

## 明 細 書

### データの加工方法及びデータのリード方法

#### 技術分野

- [0001] 本発明は、CD、DVD等の記録媒体、インターネット回線、電話回線等を通じてユーザに配布／配信されたデータ(デジタルコンテンツ)の不正使用を防止することが可能なデータの加工方法、この加工方法により加工されたデータをリードするデータのリード方法、これらの方法を実現するプログラムが記録された記録媒体に関する。

#### 背景技術

- [0002] この種の従来例として次のようなシステムが提案されている。同システムは、暗号化されたデジタルコンテンツが記録されたCD-ROM等の流通用記録媒体と、ユーザのデジタルコンテンツの使用による課金を管理するための管理手段と、流通用記録媒体を入手したユーザによりデジタルコンテンツを再生する際に使用される装置であり且つ管理手段にインターネット回線を介して接続可能なデジタルコンテンツ再生装置とを備えており、ユーザにより認証及び課金を条件としたデジタルコンテンツの再生の申し込みがデジタルコンテンツ再生装置に入力されると、デジタルコンテンツ再生装置がこの申し込みをインターネット回線を介して管理手段に送信し、管理手段が当該申し込みに係るユーザの認証及び課金を確認した上で復号鍵データをインターネット回線を介してデジタルコンテンツ再生装置に送信し、デジタルコンテンツ再生装置が復号鍵データを用いて流通用記録媒体上のデジタルコンテンツを復号化して再生する基本構成となっている(例えば、特許文献1等参照)。

- [0003] 特許文献1:特開2002-334172号公報

- [0004] しかしながら、上記従来例による場合、デジタルコンテンツ再生装置において、流通用記録媒体上のデジタルコンテンツが一度復号化されると、デジタルコンテンツの再生だけでなくコピーが簡単に行えることから、二次的な不正使用を防止することができないという本質的な欠点がある。

- [0005] ただ、再生の申し込みから所定期間が経過すると、デジタルコンテンツを自動的に削除するという機能を付加すれば、二次的な不正使用を防止することが一応可能で

あるものの、二次的使用による課金の回収をもはや期待することができないという別の欠点がある。

[0006] これはデジタルコンテンツを流通用記録媒体を通じてユーザに配付した場合だけの特有の問題ではなく、インターネット回線等を通じてユーザにデジタルコンテンツを配信した場合も同様である。即ち、コンテンツホルダー等の本来得られるべき利益が不当に損なわれ、この点でデジタルコンテンツの流通の促進が妨げられているというのが現状である。

[0007] 本発明は上記した背景の下で創作されたものであり、その第1の目的は、データ(デジタルコンテンツ)の不正使用を防止し、第2の目的はデータの二次的使用による課金の回収を確実に行うことが可能なデータの加工方法、この加工方法により加工されたデータをリードするデータのリード方法、これらの方法を実現するプログラムが記録された記録媒体を提供することにある。

#### 発明の開示

#### 発明が解決しようとする課題

[0008] 上記課題を解決するために、本発明のデータの不正使用防止方法は、暗号化されており且つ復号化ビット長毎に複合化され、これによりリードされるデータの加工方法において、データを暗号化し、このデータの復号化ビット長と異なるビット長の一部を欠落させ、その欠落部分の間を詰めて当該データを連続させたことを特徴としている。

[0009] 前記データを暗号化する前に、圧縮することができる。前記データの欠落部分の間を詰めて連続させた後、当該データの後端に欠落データと同じビット長のダミーデータを付加することが好ましい。

[0010] 欠落データのビット長は復号化ビット長の約数と異なるビット長とする。

[0011] データを複数箇所欠落させた場合、欠落データのビット長×欠落箇所数は、復号化ビット長の約数と異なるビット長とする。

[0012] 本発明のデータのリード方法は、前記データの加工方法により加工され、且つ記録媒体又はデータリード装置の補助記憶部に予め記録されたデータをデータリード装置を用いてリードするデータのリード方法であって、欠落データと当該欠落データが

データのどの部分であるかを示す位置情報とが予め記録された補助記憶装置を有する電子機器と、この電子機器と通信回線を介して接続された前記データリード装置とを備えるシステムであって、データリード装置は操作入力に応じてリードするデータに係る欠落データ及びその位置情報を電子機器に通信回線を介して要求し、電子機器は当該要求に応じて欠落データ及びその位置情報を同時又は相前後して送信し、データリード装置は欠落データ及びその位置情報を受信して補助記憶部に記録し、その後、記録媒体又は補助記憶部上のデータを主記憶部に順次転送し、主記憶部上のデータを復号化ビット長毎に順次復号化してリードするに当たり、補助記憶部上の位置情報を主記憶部に転送し、当該位置情報を参照して前記データの欠落部分を認識し、補助記憶部上の欠落データを主記憶部に転送する一方、記録媒体又は補助記憶部上のデータを当該主記憶部に転送し、当該主記憶部上でデータの当該欠落部分に当該欠落データを結合し、当該データを復号化ビット長毎に復号化するようにしたことを特徴としている。

[0013] 前記データが暗号化する前に、圧縮されている場合には、データリード装置は操作入力に応じてリードするデータに係る欠落データ及びその位置情報を電子機器に通信回線を介して要求し、電子機器は当該要求に応じて欠落データ及びその位置情報を同時又は相前後して送信し、データリード装置は欠落データ及びその位置情報を受信して補助記憶部に記録し、その後、記録媒体又は補助記憶部上のデータを主記憶部に順次転送し、主記憶部上のデータを復号化ビット長毎に順次復号化し、当該データを圧縮状態から元の状態に復元してリードするに当たり、補助記憶部上の位置情報を主記憶部に転送し、当該位置情報を参照して前記データの欠落部分を認識し、補助記憶部上の欠落データを主記憶部に転送する一方、記録媒体又は補助記憶部上のデータを当該主記憶部に転送し、当該主記憶部上でデータの当該欠落部分に当該欠落データを結合し、当該データを復号化ビット長毎に復号化し、当該データを圧縮状態から元の状態に復元するようにしている。

[0014] 前記電子機器は、欠落データ及び位置情報の送信によりデータの使用を管理する管理手段とすることができる。

[0015] 記録媒体又はデータリード装置の補助記憶部に記録されたデータは、電子機器の

前記補助記憶装置又は別の補助記憶装置に予め記録されており、データリード装置の電子機器に対する通信回線を介した要求に応じて電子機器から送信され、前記データリード装置の補助記憶部に記録される。

[0016] 前記データを所定期間リード可能とする場合には、データリード装置に欠落データを受信した時点からの経過期間を求めさせ、当該経過期間が所定期間に達したときは、少なくとも補助記憶部上の欠落データを削除させるようにすることが好ましい。

[0017] データリード装置に、欠落データとは別にデータを受信した時点からの経過期間を求めさせ、当該経過期間が所定期間に達したときは、補助記憶部上のデータを削除させることも可能である。

#### 発明の効果

[0018] 本発明の請求項1に係るデータの加工方法による場合、データを暗号化し、このデータの復号化ビット長と異なるビット長の一部を欠落させ、その欠落部分の間を詰めて連続させ、欠落部分以降のデータのデータ列を、暗号化したときのデータ列(即ち、欠落させる前のデータ列)と異なるデータ列となるようにしている。よって、データをデータリード装置でリードさせるに当たり、当該データの欠落部分以降のデータを当該データリード装置の主記憶部に順次転送し、主記憶部上の当該データを復号化ビット長毎に順次復号化すると、当該データのデータ列が暗号化したときのデータ列と異なっていることから、暗号化前のデータ列に戻らず、不明な数列又は英数列に変換される。このため、欠落部分の以降のデータをリードすることができず、データの不正使用を防止することができる。

[0019] 本発明の請求項2に係るデータの加工方法による場合、データが暗号化される前に、圧縮されている。このようなデータは、データリード装置の主記憶部に転送され、復号化ビット長毎に復号化され、そして、圧縮状態から元の状態に復元される。前記データの欠落部分以降のデータは複合化時に不明な数列又は英数列に変換されるので、この不明な数列又は英数列を圧縮状態から元の状態に復元しようとする、データリード装置のデータの復元処理が止まる。よって、データの不正使用を防止する上でメリットがある。

[0020] 本発明の請求項3に係るデータの加工方法による場合、前記データの欠落部分の

間を詰めて連続させた後、当該データの後端に欠落データと同じビット長のダミーデータを付加するようにしている。即ち、前記データのデータ長を欠落データを欠落させる前と欠落させた後とで同じとしている。これにより、第3者には前記データが一部欠落しているか否かわからない。よって、データの不正使用を防止する上でメリットがある。

- [0021] 本発明の請求項4に係るデータの加工方法による場合、欠落データのビット長を復号化ビット長の約数と異なるビット長としている。欠落データのビット長が復号化ビット長の約数であると、データリード装置の主記憶部に転送された欠落部分以降のデータのデータ列が暗号化したときのデータ列(即ち、欠落させる前のデータ列)と同じデータ列となり、これにより欠落部分の以外のデータがリード可能になるので、これを防止することができる。
- [0022] 本発明の請求項5に係るデータの加工方法による場合、欠落データのビット長×欠落箇所数は、復号化ビット長の約数と異なるビット長となっている。よって、欠落データのビット長×欠落箇所数が復号化ビット長の約数であると、データリード装置の主記憶部に転送された欠落部分以降のデータのデータ列が暗号化したときのデータ列(即ち、欠落させる前のデータ列)と同じデータ列となり、これにより欠落部分の以外のデータがリード可能になるので、これを防止することができる。
- [0023] 本発明の請求項6に係るデータのリード方法による場合、電子機器の補助記憶装置に記録された欠落データ及びその位置情報を、データリード装置に要求させ、当該データリード装置の補助記憶部に記録させておき、その後、データリード装置に記録媒体又は補助記憶部上のデータをリードさせるに当たり、前記位置情報を参照させてデータの欠落部分を認識させ、補助記憶部上の欠落データと記録媒体又は補助記憶部上のデータと主記憶部に転送させ、データの当該欠落部分に欠落データを結合させ、主記憶部上の当該データを復号化ビット長毎に復号化させ、当該データをリードさせるようにしている。このようにデータの欠落部分に欠落データを結合させることにより、欠落部分前後のデータ列が暗号化したときのデータ列に戻る。このため、欠落部分前後のデータを復号化させても不明な数列又は英数列に変換されないで、データのリードが可能になる。即ち、欠落させた欠落データを真正の使用者

として得ない限り、データをリードすることができないので、データの不正使用を防止することができる。しかも、記録媒体に記録されたデータが単純にコピーされたとしても当該データをリードするためには真正の利用者として欠落データを得ることが必要になる。よって、ここに二次的、三次的利用による課金の回収を確実に行うことが可能になる。

[0024] 本発明の請求項7に係るデータのリード方法による場合、電子機器の補助記憶装置に記録された欠落データ及びその位置情報を、データリード装置に要求させ、当該データリード装置の補助記憶部に記録させておき、その後、データリード装置に記録媒体又は補助記憶部上のデータをリードさせるに当たり、前記位置情報を参照させてデータの欠落部分を認識させ、補助記憶部上の欠落データと記録媒体又は補助記憶部上のデータと主記憶部に転送させ、当該データの欠落部分に当該欠落データを結合させ、主記憶部上の当該データを復号化ビット長毎に復号化させ、当該データを圧縮状態から元の状態に復元してリードさせるようにしている。このようにデータの欠落部分に欠落データを結合させることにより、欠落部分前後のデータ列が暗号化したときのデータ列に戻る。このため、欠落部分前後のデータを復号化させても不明な数列又は英数列に変換されないため、復元処理がストップせず、データのリードが可能になる。即ち、欠落データを真正の利用者として得ない限り、データをリードすることができないので、データの不正使用を防止することができる。しかも、記録媒体に記録されたデータが単純にコピーされたとしても当該データをリードするためには真正の利用者として欠落データを得ることが必要になる。よって、ここに二次的、三次的利用による課金の回収を確実に行うことが可能になる。

[0025] 本発明の請求項8記載のデータのリード方法による場合、前記電子機器は、欠落データ及び位置情報の送信によりデータの利用を管理する管理手段である。よって、データの利用に応じて課金等が可能になる。

[0026] 本発明の請求項9記載のデータのリード方法による場合、データリード装置の記録媒体又は補助記憶部に記録されたデータは、電子機器の前記補助記憶装置又は別の補助記憶装置に予め記録されており、データリード装置の電子機器に対する通信回線を介した要求に応じて電子機器から送信され、前記データリード装置の記録媒

体又は補助記憶部に記録されるようになっている。このため、データの入手が簡単になる。

[0027] 本発明の請求項10記載のデータのリード方法による場合、データリード装置に欠落データを受信した時点からの経過期間を求めさせ、当該経過期間が所定期間に達したときは、送信された欠落データを削除させるようにしたので、データの不正な二次的使用を防止することができる。

[0028] 本発明の請求項11に係るデータのリード方法による場合、データリード装置に、欠落データとは別にデータを受信した時点からの経過期間を求めさせ、当該経過期間が所定期間に達したときは、送信されたデータを削除させるようにしたので、データが所定期間以上データリード装置内に残ることがない。よって、不正目的でのデータのコピーを防止する上でメリットがある。

[0029] 本発明の請求項12に係る記録媒体による場合、請求項1乃至5と同様の効果を得ることができる。本発明の請求項13に係る記録媒体による場合、請求項6乃至11と同様の効果を得ることができる。

#### 図面の簡単な説明

[0030] [図1]本発明の第1の実施の形態を説明するための図であって、デジタルコンテンツの不正使用防止システムの構成図であって、同システムに使用される流通用記録媒体作成装置の構成図を含んだ図である。

[図2]同システムに用いられる再生用ソフトウェアのフローチャートである。

[図3]同システムの管理センタの制御部により処理されるユーザ登録用割込プログラムのフローチャートである。

[図4]同管理センタの制御部により処理されるピースデータ配信用割込プログラムのフローチャートである。

[図5]同システムに用いられる流通用記録媒体作成装置であるコンピュータにより実行される記録媒体作成用ソフトウェアのフローチャートである。

[図6]本発明の第2の実施の形態に係るデジタルコンテンツの不正使用防止システムの構成図である。

[図7]同システムに使用される再生用ソフトウェアのフローチャートである。

[図8]同システムの配信管理センタの制御部により処理されるユーザ登録割込プログラムのフローチャートである。

[図9]同システムの配信管理センタの制御部により処理されるピースデータ配信用割込プログラムである。

[図10]本発明の第3の実施の形態に係るデジタルコンテンツの不正使用防止システムの構成図である。

[図11]デジタルコンテンツの不正使用防止システムに使用される再生用ソフトウェアのフローチャートである。

[図12]コンテンツダウンロード用割込プログラムのフローチャートである。

[図13]本発明の第4の実施の形態に係るデジタルコンテンツの不正使用防止システムの構成図である。

[図14]同システムに使用される再生用ソフトウェアのフローチャートである。

[図15]同システムのコンテンツファイルを示す図であって、(a)がデータ本体のイメージ図、(b)がデータ本体の $\alpha$ 部分のイメージ図である。

[図16]同システムに用いられる流通用記録媒体作成装置であるコンピュータにより実行される記録媒体作成用ソフトウェアのフローチャートである。

[図17]本発明の第5の実施の形態に係るデジタルコンテンツの不正使用防止システムの構成図である。

[図18]同システムに使用される再生用ソフトウェアのフローチャートである。

## 符号の説明

[0031]  $\alpha$  流通用記録媒体

100 デジタルコンテンツの不正使用防止システム

110 管理センタ

120 デジタルコンテンツ再生装置

140 流通用記録媒体作成装置

200、300、デジタルコンテンツの不正使用防止システム

210、310 配信管理センタ

220、320 デジタルコンテンツ再生装置



400 デジタルコンテンツの不正使用防止システム

410 管理センタ

420 デジタルコンテンツ再生装置

500、デジタルコンテンツの不正使用防止システム

510 配信管理センタ

520 デジタルコンテンツ再生装置

発明を実施するための最良の形態

[0032] 以下、本発明の実施の形態を説明する。

#### 実施例 1

[0033] まず、本発明の第1の実施の形態を図1及び図2を参照して説明する。図1はデジタルコンテンツの不正使用防止システムの構成図であって、同システムに使用される流通用記録媒体作成装置の構成図を含んだ図、図2は同システムに用いられる再生用ソフトウェアのフローチャート、図3は同システムの管理センタの制御部により処理されるユーザ登録用割込プログラムのフローチャート、図4は同管理センタの制御部により処理されるピースデータ配信用割込プログラムのフローチャートである。

[0034] 図1に示すデジタルコンテンツの不正使用防止システム100は、ユーザにレンタルを目的として配布された流通用記録媒体 $\alpha$ 上のコンテンツファイルが不正使用されるのを防止するシステムである。なお、レンタルの対象であるのはコンテンツファイルであり、流通用記録媒体 $\alpha$ 自体ではない。

[0035] 同システムは、ヘッダ情報a及びデータ本体bを有したコンテンツファイルがデータ本体bの一部(欠落データ)を欠落させた状態で記録された流通用記録媒体 $\alpha$ と、流通用記録媒体 $\alpha$ 上のコンテンツファイルの利用を管理する管理手段であって、欠落データ及び当該欠落データがデータ本体bのどの部分であるかを示す位置情報からなるピースデータdとが予め用意されており且つ当該ピースデータdを通信回線 $\beta$ を介して配信可能な管理センタ110(電子機器)と、流通用記録媒体 $\alpha$ 上のコンテンツファイルを再生及びコピーする際に使用される装置であって管理センタ110との間で通信回線 $\beta$ を介して通信可能な機能を有したデジタルコンテンツ再生装置120(データリード装置)とを備えた基本構成となっている。

- [0036] 通信回線 $\beta$ については光通信回線等のデジタル回線や電話回線等のアナログ回線等の有線又は無線のインターネット回線、又はデジタル放送、衛星放送等の電波信号の送受信を行う回線であり、これを用いて管理センタ110とデジタルコンテンツ再生装置120との間で相互通信を行うようにしている。
- [0037] 流通用記録媒体 $\alpha$ はCD、DVD等の一般的な記録媒体である。流通用記録媒体 $\alpha$ 上のコンテンツファイルは、音楽、動画、静止画、テキスト、ゲーム又はソフトウェア等のデータであるデータ本体b(データ)と、このデータ本体bを再生するための再生情報及びデータ本体bに割り当てられたコンテンツID、管理センタ110のWEBアドレスの情報等のコンテンツ情報を含むヘッダ情報aとを有し、ヘッダ情報a及びデータ本体bがそれぞれ暗号化された後、当該データ本体bの一部が欠落したデータ構造となっている。なお、データ本体bの最初の部分には、当該データ本体bの開始位置を示す開始位置情報が記録されている。欠落データがデータ本体bのどの部分であるかを示す位置情報とは開始位置情報から欠落部分までのデータ長や時間のことである。再生情報とは最初に読み込むべきアドレス値等である。
- [0038] 管理センタ110はデータ本体bに含められた著作物の著作権者等との間の契約の下、流通用記録媒体 $\alpha$ 上のデータ本体bをユーザにレンタルさせるとともにそのレンタル使用料をユーザから回収するという事業を行う者が運営するサーバである。図中111はピースデータd及びコンテンツファイルのデータ本体bを復号化するのに必要な復号鍵c2とが予め記録されたピースデータDB(補助記憶装置)、112はコンピュータ等の制御部、113は通信を行うための通信部、114はユーザ情報が記録される他、これに基づく認証や課金等の情報が順次記録されるユーザ情報DB、115は再生用ソフトウェア及びコンテンツファイルのヘッダ情報aを復号化するのに必要な復号鍵c1が予め記録されたソフトウェアDB、116はハードディスク等のメモリ部である。
- [0039] メモリ部116にはサーバとしてのオペレーションシステム等の基本プログラム以外に、図3に示すユーザ登録割込プログラム、図示しない再生用ソフトウェアダウンロード用割込プログラム及び図4に示すピースデータ配信用割込プログラム等が記録されている。これらのプログラムの内容については後述するが、同プログラムが制御部112で処理されることより、同サーバが管理センタ110としての機能を発揮するようにな

っている。また、メモリ部116には、ユーザ登録処理に必要なデータや再生申込処理に必要なデータが記録されている。

- [0040] ピースデータDB111上のピースデータdには対応するコンテンツファイルを示すコンテンツIDが付加されている。このようにコンテンツIDを用いて流通用記録媒体 $\alpha$ 上のコンテンツファイルとピースデータDB111上のピースデータdとの対応関係を一致させるようにしている。同様にユーザ情報DB114上のユーザ情報には対応するユーザのユーザID及びプレーヤIDが付加されている。このようにユーザID又はプレーヤIDを用いてユーザ情報DB114におけるユーザとユーザ情報との対応関係を一致させるようにしている。
- [0041] この管理センタ110は、ピースデータdをデジタルコンテンツ再生装置120に送信する前に、ユーザID及びパスワードの確認(即ち、認証)を行う他、プレーヤIDが一致するか否かも含めて確認することから、プレーヤIDは不正使用防止にも役立つことになる。
- [0042] デジタルコンテンツ再生装置120はユーザが使用する汎用のコンピュータである。図中121はCPU等の制御部、122はモニタやスピーカ等の出力部、123はキーボードやマウス等の操作部、124は流通用記録媒体 $\alpha$ 等に対してデータのリード/ライトを行う再生複写部、125はハードディスク等のメモリ部(補助記憶部)、126は通信を行うための通信部である。
- [0043] メモリ部125にはコンピュータとしてのオペレーションシステム等の基本プログラム以外に、図2に示す再生用ソフトウェアが記録されている。この再生用ソフトウェアはユーザ登録を条件として管理センタ110から通信回線 $\beta$ を通じてダウンロードされた有償又は無償のソフトウェアであって、流通用記録媒体 $\alpha$ 上のコンテンツファイルを再生するのに必要なアプリケーションソフトである。また、メモリ部125には再生用ソフトウェアに割り当てられたプレーヤIDが当該再生用ソフトウェアと共に管理センタ110から送信され、記録される。更に、メモリ部125には管理センタ110から送信されたピースデータd、復号鍵c1、c2等が記録される他、レンタル期間などを示すレンタル情報が記録される。
- [0044] 再生用ソフトウェアの内容については後述するが、同ソフトウェアが制御部121で

処理されることより、同コンピュータがデジタルコンテンツ再生装置120としての機能を発揮するようになっている。

[0045] 以上のように構成されたデジタルコンテンツの不正使用防止システム100の動作について説明し、併せて管理センタ110の動作、デジタルコンテンツ再生装置120の動作及び各プログラムの内容について説明する。

[0046] まず、ユーザが自己のコンピュータ(デジタルコンテンツ再生装置120に相当するコンピュータであり、図2に示す再生用ソフトウェアがダウンロードされていない状態)の操作部123を操作して通信回線 $\beta$ を介して管理センタ110にアクセスし、ユーザ登録の要求を行う。管理センタ110は、この要求に応じて図3に示すユーザ登録用割込プログラムを処理し、ユーザ登録に必要なデータを前記コンピュータに向けて送信する(s21)。その後、ユーザが前記コンピュータの操作部123を通じてユーザ登録用画面が示すところに従って氏名、住所及び支払条件「自己の銀行口座番号又はクレジットカード番号等」等を入力し、この登録データを通信回線 $\beta$ を介して管理センタ110に送信する。すると、管理センタ110は、これに応じてユーザIDやパスワードを作成し、当該ユーザID等を登録データと共にユーザ情報としてユーザ情報DB114に登録する(

s22) 一方、当該ユーザIDやパスワードを通信回線 $\beta$ を介してユーザのコンピュータに送信する(s23)。そして、ユーザ登録用割込プログラムの処理を終了する。なお、ユーザIDやパスワードはユーザ登録の際にユーザ自身に入力させるようにしても良い。

[0047] その後、ユーザが自己のコンピュータを操作して、管理センタ110にアクセスし、再生用ソフトウェアのダウンロードの要求を入力する。この際、ユーザIDやパスワードが必要になる。すると、ユーザのコンピュータは、その要求を通信回線 $\beta$ を通じて管理センタ110に送信する。管理センタ110は、この要求に応じて前記再生用ソフトウェアダウンロード用割込プログラムを処理し、ソフトウェアDB115上の再生用ソフトウェア及び復号鍵c1を読み出して通信回線 $\beta$ を介してユーザのコンピュータに送信する。すると、図2に示す再生用ソフトウェアが同コンピュータのメモリ部125にダウンロードされ、インストールされる。と同時に復号鍵c1がメモリ部125に記録される。これによ

り同コンピュータがデジタルコンテンツ再生装置120となるのである。

- [0048] このデジタルコンテンツ再生装置120は、ユーザにより流通用記録媒体 $\alpha$ が再生複写部124にセットされる一方、再生用ソフトウェアの実行操作がなされると、当該再生用ソフトウェアを処理し、当該再生用ソフトウェアに含まれる再生プレーヤ及びレンタル中のコンテンツを示すプレイリストのデータを出力部122に表示出力する。すると、当該再生プレーヤの画面上にプレイリストが表示される(s1)。即ち、再生の申込がされたことを示す所定のフラグが立っているコンテンツファイルをプレイリストに表示する。そして、このプレイリストに基づき操作部123を通じて再生操作がなされたか否かを判定する(s2)。
- [0049] 再生操作がなされていないと判定すると、操作部123を通じて流通用記録媒体 $\alpha$ の読み込みの操作(DISC LOADの操作)がなされたか否かを判定する(s3)。DISC LOADの操作がなされると、再生の申し込みがされていないコンテンツファイルを示すコンテンツリストを出力部122に表示出力する(s4)。即ち、メモリ部125上の復号鍵c1を読み出す一方、流通用記録媒体 $\alpha$ 上のコンテンツファイルのうち所定のフラグが立っていないコンテンツファイルのヘッダ情報aを読み出し、当該復号鍵c1を用いてヘッダ情報aを復号化し当該ヘッダ情報aに含まれるコンテンツ情報を読み出し、コンテンツリストに表示する。
- [0050] その後、ユーザによりコンテンツリスト上のコンテンツファイルの再生の申し込みがなされると、メモリ部125上の復号鍵c1を読み出す一方、流通用記録媒体 $\alpha$ 上の当該コンテンツファイルのヘッダ情報aを読み出し、当該復号鍵c1を用いてヘッダ情報aを復号化して当該ヘッダ情報aに含まれるコンテンツ情報を読み出す。そして、当該コンテンツ情報に含まれるWEBアドレスに基づき当該コンテンツ情報に含まれるコンテンツIDを通信回線 $\beta$ を介して管理センタ110に送信する。このようにして再生申込処理を行う旨を送信する。
- [0051] すると、管理センタ110は図4に示すピースデータ配信用割込プログラムを処理する。そして、メモリ部116から再生申込処理に必要なデータを読み出し、通信回線 $\beta$ を介してデジタルコンテンツ再生装置120に送信する(s31)。デジタルコンテンツ再生装置120は、このデータに基づいて再生申込用画面を出力部122に表示出力す

る(s5)。

- [0052] その後、ユーザが再生申込用画面が示すところに従ってレンタル期間を操作部123を通じて順次入力又は選択(これによりレンタル金額が決まる)し、最後にユーザIDやパスワードを流通用記録媒体 $\alpha$ の再生申し込みとして操作部123を通じて入力すると(s6)、デジタルコンテンツ再生装置120は、出力部122の表示出力を認証画面に切り換える一方、入力された申し込みデータを通信回線 $\beta$ を介して管理センタ110に送信する。この際、流通用記録媒体 $\alpha$ 上のヘッダ情報aのコンテンツ情報に含まれるコンテンツID及びメモリ部125上のプレーヤIDを読み出し、申し込みデータと一緒に管理センタ110に送信する(s7)。
- [0053] すると、管理センタ110は、申し込みに係るユーザの認証を確認する(s32)。即ち、送信されたユーザのユーザIDやプレーヤID等を参照してユーザ情報DB114から当該ユーザのユーザ情報を読み出し、当該ユーザが真正のユーザであるか否かを確認する。このとき、管理センタ110は、ユーザ情報DB114にレンタル料金の不払い等が所定以上ある不適当者リストが予め用意されており、当該認証と共に不適当者リストに該当する者でないか否かを確認する(この不適当者リストの確認は任意である)。
- [0054] 管理センタ110は、申し込みに係るユーザが不正なユーザである又は真正のユーザであるものの不適当者リストに該当する者であると確認した場合、ユーザの申し込みを拒否する旨を通信回線 $\beta$ を介してデジタルコンテンツ再生装置120に送信する(s33)。そして、ピースデータ配信用割込プログラムを処理を終了する。
- [0055] 一方、申し込みに係るユーザが真正のユーザであり且つ不適当者リストに該当しない者であることを確認した場合、ユーザのプレーヤID等を参照して当該ユーザのユーザ情報DB114上のユーザ情報に課金を記録する一方、コンテンツIDを参照してピースデータDB111を検索し当該コンテンツIDに対応する復号鍵c2及びピースデータdを読み出し、これを申し込みデータに含まれるレンタル期間等を示すレンタル情報と共にユーザの申し込みを承諾する旨の回答として通信回線 $\beta$ を介してデジタルコンテンツ再生装置120に送信する(s34)。そして、ピースデータ配信用割込プログラムを処理を終了する。

- [0056] なお、課金については、所定期間毎にユーザ情報DB114に基いて集計し、銀行・カード会社130に請求するか若しくは、ユーザに直接請求してユーザに振込やコンビニエンスストア等で支払いをさせるようにする。また、管理センタ110が銀行・カード会社130と通信回線 $\beta$ を介して接続されている場合には、即時決済とすることももちろん可能である。
- [0057] デジタルコンテンツ再生装置120は、その後、通信回線 $\beta$ を介してユーザの申し込みを拒否する旨を受信すると(s8)、エラーメッセージを出力部122に表示出力する(s9)。一方、通信回線 $\beta$ を介してピースデータd等を受信すると(a8)、所定のフラグを立てる一方、復号鍵c2、ピースデータd及びレンタル情報をメモリ部125に記録する(s10)。と同時に、コンピュータの時計機能を用いてピースデータ送信日時をメモリ部125に記録する。そして、プレイリストを更新して出力部122に表示出力し、当該プレイリスト中にピースデータdを得たコンテンツファイルのファイル名を表示させる(s1)。
- [0058] その後、デジタルコンテンツ再生装置120は、操作部123を通じてプレイリストに基づきコンテンツファイルの再生操作がなされると(s2)、メモリ部125上の復号鍵c1を読み出す一方、流通用記録媒体 $\alpha$ 上の当該コンテンツファイルに係るヘッダ情報aを読み出し当該復号鍵c1を用いてヘッダ情報aを復号化する。そして、当該ヘッダ情報aに含まれる再生情報を用いて流通用記録媒体 $\alpha$ 上のデータ本体bを読み出し、当該データ本体bをメモリ部125上の復号鍵c2で復号化しつつ再生する(s11)。と共に、流通用記録媒体 $\alpha$ 上のデータ本体bの開始位置情報を読み出す一方、メモリ部125上のピースデータdを読み出し、開始位置情報からピースデータdに含まれる位置情報までのデータ長や時間のカウントを開始する(s12)。その後、前記カウントが終了したか否かを判定する(s13)これにより、データ本体bの欠落部分の認識を行う。この判定の結果、カウントが終了したと判定しデータ本体bの欠落部分を認識すると、メモリ部125上のピースデータdを読み出し、当該ピースデータdに含まれる欠落データを当該データ本体bの欠落部分のデータとして読み出しメモリ部125上の復号鍵c2で復号化しつつ再生する(s14)。その後、再び流通用記録媒体 $\alpha$ 上のデータ本体bを読み出しメモリ部125上の復号鍵c2で復号化しつつ続きの再生を行う(s15)。なお、この再生用ソフトウェア

のプログラムはユーザにより終了の処理が行われることにより終了する。

[0059] また、再生用ソフトウェアには、上述した基本機能の他、デジタルコンテンツ再生装置120の電源がONにされると、デジタルコンテンツ再生装置120に常駐し、ピースデータdの管理を行うピースデータ管理機能を有している。このピースデータ管理機能においては、メモリ部125上のピースデータdの管理を行う一方、ピースデータ送信日時と現在の日時との差をピースデータdが送信された時点からの経過期間として求め、これがレンタル情報に含まれるレンタル期間に達しているときはレンタル期間外であるとしてメモリ部125上のピースデータd及び復号鍵c2を削除する一方、所定のフラグを倒すようになっている。

[0060] このように同システム100においては、ユーザがデジタルコンテンツ再生装置120を使用して流通用記録媒体 $\alpha$ を再生操作しても、真正の再生の申込者として管理センタ110からピースデータdを得ない限り、流通用記録媒体 $\alpha$ 上のコンテンツファイルのデータ本体bを再生することができない。このようにして流通用記録媒体 $\alpha$ 上のコンテンツファイルの一時的な不正使用を防止することができる。しかも、レンタル期間が過ぎたものについては、ピースデータdが削除されるので、二次的な不正使用も防止することができる。さらに、ユーザにより流通用記録媒体 $\alpha$ が他の流通用記録媒体にコピーされたとしても、他の流通用記録媒体に記録されたコンテンツファイルにはヘッダ情報aに含まれる再生情報が欠落していることから、真正の再生の申込者としてピースデータdを得ない限り、再生することができない。よって、三次的な不正使用も防止することができる。

[0061] また、流通用記録媒体 $\alpha$ のレンタル期間外においてはメモリ部125上のピースデータd等が自動的に削除されるだけで、流通用記録媒体 $\alpha$ 上のコンテンツファイルはそのままである。デジタルコンテンツ再生装置120を使用してコンテンツファイルを新たな記録媒体に流通用記録媒体 $\alpha$ をコピーにより作成することも可能である。このような流通用記録媒体 $\alpha$ 上のコンテンツファイルを再生するには、デジタルコンテンツ再生装置120を使用して、管理センタ110に対する認証及びレンタル使用料の支払いが必要になるので、ここに二次的、三次的使用による課金の回収を確実に行うことが可能になる。



- [0062] しかも、流通用記録媒体 $\alpha$ とは別に、再生の申込においてコンテンツファイルデータ本体bに係る課金の回収を行う仕組みになっているので、流通用記録媒体 $\alpha$ を無料で配布し、その後再生の申込をした者に対して課金を行ったり、流通用記録媒体 $\alpha$ をこれに係る代金のみで販売し、その後再生の申込をした者に対して課金を行うようにしたりすることもできる。また、流通用記録媒体 $\alpha$ に記録されたコンテンツファイルの内容が医学書等の専門書である場合、医学書等の専門書の内容を各項目に分割し、各々の項目を一コンテンツファイルとして流通用記録媒体 $\alpha$ に記録し、各項目毎に再生の申込を行うようにすることができる。このようにすれば高価な専門書であっても各家庭に常備することができ、必要に応じて項目毎に再生の申込(レンタル)をして参照することができる。このように同システムを用いれば、各種の新規なビジネスの形態に対応することができる。
- [0063] さらに、流通用記録媒体 $\alpha$ に複数のコンテンツファイルが記録されている場合には、ユーザにとっては視聴したいコンテンツファイルのみをレンタルすることができる。一方、流通用記録媒体 $\alpha$ を作成する者にとっては各ユーザの好みや流行等を考慮せず任意のコンテンツファイルが記録された流通用記録媒体 $\alpha$ に作成することができるので、当該流通用記録媒体 $\alpha$ の作成コストの低減を図ることができる。
- [0064] ここで流通用記録媒体 $\alpha$ を作成するのに使用される流通用記録媒体作成装置140について図1及び図5を参照して説明する。図5は同システムに用いられる流通用記録媒体作成装置であるコンピュータにより実行される記録媒体作成用ソフトウェアのフローチャートである。
- [0065] 流通用記録媒体作成装置140は、管理センタ110の事業者又はこれに関係する者が使用する装置であって、ヘッダ情報aとデータ本体bとを有したコンテンツファイルから当該データ本体bの一部を分離し、当該欠落データとその位置情報とをピースデータdとして記録する一方、ピースデータdを分離したコンテンツファイルをセットされた記録媒体に記録して流通用記録媒体 $\alpha$ を作成する構成となっている。ここではコンピュータを用いている。
- [0066] 図1中141は、マスターディスクからデジタルコンテンツを読み出す入力部、142は図5に示す記録媒体作成用ソフトウェアを処理するCPU等の制御部、143はCD、D

VD等の記録媒体がセットが可能であり同記録媒体にコンテンツファイルを記録する記録部、144はコンテンツファイルから分離されたピースデータdを記録するピースデータ用メモリ、記録媒体作成用ソフトウェアが記録されたハードディスク等のメモリ部145である。

[0067] 以下、図5に示す記録媒体作成用ソフトウェアの内容について説明し、併せて流通用記録媒体作成装置140の動作について説明する。

[0068] 流通用記録媒体作成装置140は電源がONにされると、メモリ部145上の記録媒体作成用ソフトウェアを処理する。そして、入力部141にはマスターディスクが手動又は自動的にセットされる。また、記録部143にはDVD等の記録媒体が自動的に順次セットされるようになっている。

[0069] まず、入力部141によりセットされたマスターディスクからコンテンツファイルを読み出し(s1)、当該コンテンツファイルのヘッダ情報aとデータ本体bとを各々暗号化する(s2)。その後、コンテンツファイルに含まれるデータ本体bの一部を分離し、分離した当該欠落データをその位置情報と共にピースデータdとしてピースデータ用メモリ144に記録する(s3)。一方、当該コンテンツファイルを記録部143にセットされたDVD等の記録媒体に記録する(s4)。これで同ソフトウェアが終了となる。なお、ピースデータ用メモリ144に記録されたピースデータdは通信回線βを介して管理センタ110へ転送される。このようにして流通用記録媒体aが作成される。なお、ピースデータ用メモリ144に記録されたピースデータdを記録媒体に記録して管理センタ110に送ることもできる。

[0070] 以上のようなデジタルコンテンツの不正使用防止システム100については、ヘッダ情報とデータ本体とを有したコンテンツファイルがデータ本体の一部を欠落させた状態で記録された流通用記録媒体と、流通用記録媒体上のコンテンツファイルの利用を管理する手段であって前記欠落データ及び当該欠落データがデータ本体のどの部分であるかを示す位置情報が記録されたデータベースを有し、当該欠落データ及びその位置情報を通信回線を介して送信可能な管理手段と、流通用記録媒体上のコンテンツファイルを少なくとも再生する際に使用される装置であって管理手段との間で通信回線を介して通信可能な機能を有したデジタルコンテンツ再生装置とを備

え、ユーザによりコンテンツファイルの再生の申し込みがデジタルコンテンツ再生装置に入力されると、デジタルコンテンツ再生装置が当該申し込みを通信回線を介して管理手段に送信し、管理手段が当該申し込みに係るコンテンツファイルの欠落データ及びその位置情報を同時又は相前後して通信回線を介して当該デジタルコンテンツ再生装置に送信し、デジタルコンテンツ再生装置は当該欠落データと位置情報を同時又は相前後して受信してメモリ部に記録し、流通用記録媒体上のコンテンツファイルのデータ本体を読み出して再生すると共に、メモリ部から読み出した位置情報を参照して前記データ本体の欠落部分を認識し、メモリ部上の欠落データを当該欠落部分のデータとして読み出して再生する構成となっている限りどのような設計変形を行ってもかまわない。

[0071] よって、流通用記録媒体 $\alpha$ については、ヘッダ情報a及びデータ本体bが各々暗号化されているとしたが、暗号化するか否かは任意である。ただ、少なくともデータ本体bが暗号化されていることが望ましい。また、コンテンツファイルはヘッダ情報a及びデータ本体bを有する構成であるとしたが、その他の情報を付加した状態で記録することは勿論可能である。その他の情報としては、ユーザのコンピュータに再生用ソフトウェアがインストールされているか否かを判断して、インストールされていないと判断した場合には、管理センタ110のHPに自動的にアクセスするプログラム等がある。このプログラムを記録させておくと、ユーザが自己のコンピュータ(デジタルコンテンツ再生装置120に相当するコンピュータであり、再生用ソフトウェアがダウンロードされていない状態)に予め入手した流通用記録媒体 $\alpha$ をセットすると、管理センタ110のWEBアドレスを読み出し、これに基づいて管理センタ110にアクセスする。その後、上述した手順で再生用ソフトウェアを入手することができる。なお、コンテンツファイルについては、一部が欠落しているとしたが、複数箇所を欠落させることも当然可能であることは言うまでもない。

[0072] 位置情報については、開始位置情報から欠落部分までのデータ長や時間であるとしたが、欠落部分を示すアドレス値等であっても良い。この場合、次に読み出すべき流通用記録媒体 $\alpha$ 上のデータ本体bのアドレス値と位置情報とが一致するか否かを逐次判定し、この判定の結果、一致しないと判定したときには前記アドレス値の示す

流通用記録媒体  $\alpha$  上のデータ本体  $b$  を読み出し、一致すると判定したときにはメモリ部125上の欠落データを読み出すようにする。

[0073] ピースデータ  $d$  については、欠落データ本体とその位置情報とからなるとしたが、前記位置情報を含めるか否かは任意である。この場合、例えば、予めデータ本体  $b$  の欠落部分の前に欠落部分であることを示す欠落位置情報を記録しておき、データ本体  $b$  を再生すると共に、開始位置情報から欠落位置情報までをカウントし、このカウントが終了すると、メモリ部125上の欠落データを当該欠落部分のデータとして再生するようにすれば良い。或いは、予めデータ本体  $b$  の欠落部分の位置を決定しておく一方、再生用ソフトウェアに欠落させた欠落データの位置情報が予め用意しておく。そして、データ本体  $b$  を再生すると共に、この位置情報に基づいてデータ本体  $b$  の欠落部分を認識し、メモリ部125上の欠落データを当該欠落部分のデータとして再生するようにすることもできる。

[0074] このように再生用ソフトウェアの内容については、一例に過ぎず、同様の内容を実現可能である限りどのような設計変形を行ってもかまわない。ユーザ登録用割込プログラム、再生用ソフトウェアダウンロード用割込プログラム及びピースデータ配信用割込プログラムについても同様である。

[0075] なお、第1の実施の形態については、レンタルではなく有償又は無償でユーザに譲渡された流通用記録媒体  $\alpha$  上のコンテンツファイルの不正使用を防止するシステムに設計変更することも可能であり、この場合であっても上記と同様のメリットを奏する。この場合に使用される再生用ソフトウェアについては、レンタル期間の内外に応じた一連の処理を削除するだけの内容で良い。また、デジタルコンテンツ再生装置に関しては、再生用ソフトウェアを管理センタ110からダウンロードするのではなく、CD等の記録媒体を通じてインストールするようにしても良い。また、コンピュータではなく専用装置とすることも可能であるのは当然であり、ユーザにより認証及び課金を条件としたコンテンツファイルの再生の申し込みが入力されると、当該申し込みを通信回線  $\beta$  を介して管理センタ110に送信し、その後、管理センタ110からピースデータ  $d$  が通信回線  $\beta$  を介して送信されると、再生操作時に流通用記録媒体  $\alpha$  上のヘッダ情報及び当該ピースデータ  $d$  を用いて流通用記録媒体  $\alpha$  上のデータ本体  $b$  を再生する

という機能を有する限り、どのような構成のものを用いてもかまわない。

## 実施例 2

- [0076] 次に、本発明の第2の実施の形態を図面を参照しつつ説明する。図6はデジタルコンテンツの不正使用防止システムの構成図、図7は同システムに使用される再生用ソフトウェアのフローチャート、図8は同システムの配信管理センタの制御部により処理されるユーザ登録割込プログラムのフローチャート、図9は同システムの配信管理センタの制御部により処理されるピースデータ配信用割込プログラムである。
- [0077] 図7に示すデジタルコンテンツ(データ)の不正使用防止システム200は、ユーザにレンタルを目的として配信されたコンテンツファイルが不正使用されるのを防止するシステムである。
- [0078] 同システムは、ヘッダ情報aとデータ本体bとを有したコンテンツファイルがヘッダ情報a及びデータ本体bがデータ本体bの一部を欠落させた状態で予め用意されると共に、欠落データ及び当該欠落データがデータ本体bのどの部分であるかを示す位置情報からなるピースデータdが当該コンテンツファイルとは別に予め用意されたサーバであって、当該コンテンツファイルを通信回線 $\beta$ (実施例1と同じ)を介して配信する一方、当該データ本体bの利用を管理する配信管理手段としての配信管理センタ210(電子機器)と、配信管理センタ210との間で通信回線 $\beta$ を介して通信可能であり且つ配信管理センタ210から配信されたコンテンツファイルを再生及びコピーする際に使用されるデジタルコンテンツ再生装置220(データリード装置)とを備えた構成となっている。
- [0079] ここでいうコンテンツファイルは、音楽、動画、静止画、テキスト、ゲーム又はソフトウェア等のデータであるデータ本体bと、このデータ本体bを再生するための再生情報及びデータ本体bに割り当てられたコンテンツID、配信管理センタ210のWEBアドレスの情報等のコンテンツ情報を含むヘッダ情報aとを有し、ヘッダ情報a及びデータ本体bがそれぞれ暗号化された後、当該データ本体bの一部が欠落したデータ構造となっている。なお、データ本体bの最初の部分には、当該データ本体bの開始位置を示す開始位置情報が記録されている。欠落データがデータ本体bのどの部分であるかを示す位置情報とは開始位置情報から欠落部分までのデータ長や時間のことで

ある。

[0080] 配信管理センタ210は配信すべきコンテンツファイルのデータ本体bに含められた著作物の著作権者等との間の契約の下、コンテンツファイルをユーザにレンタルさせるとともにその使用料をユーザから回収するという事業を行う者が運営するサーバである。図中211はヘッダ情報aとデータ本体bとを有したコンテンツファイルがヘッダ情報a及びデータ本体bがデータ本体bの一部を欠落させた状態で予め記録されたデジタルコンテンツDB(補助記憶装置)、212はコンピュータ等の制御部、213は通信を行うための通信部、214はユーザ情報が記録される他、これに基づく認証や課金等の情報が順次記録されるユーザ情報DB、215は再生用ソフトウェア及びコンテンツファイルのヘッダ情報aを復号化するのに必要な復号鍵c1が予め記録されたソフトウェアDB、216はピースデータd及びコンテンツファイルのデータ本体bを復号化するのに必要な復号鍵c2が予め記録されたピースデータDB、217はハードディスク等のメモリ部である。

[0081] メモリ部217にはサーバとしてのオペレーションシステム等の基本プログラム以外に、図8に示すユーザ登録割込プログラム、図示しない再生用ソフトウェアダウンロード用割込プログラム、図示しないコンテンツダウンロード用割込プログラム及び図9に示すピースデータ配信用割込プログラム等が記録されている。これらのプログラムの内容については後述するが、同プログラムが制御部212で処理されることより、同サーバが配信管理センタとしての機能を発揮するようになっている。また、メモリ部217には、ユーザ登録処理に必要なデータや再生申込処理に必要なデータが記録されている。

ピースデータDB216上のピースデータdには対応するコンテンツファイルを示すコンテンツIDが付加されている。このようにコンテンツIDを用いてコンテンツファイルとピースデータDB216上のピースデータdとの対応関係を一致させるようにしている。同様にユーザ情報DB214上のユーザ情報には対応するユーザのユーザID及びプレーヤIDが付加されている。このようにユーザID又はプレーヤIDを用いてユーザ情報DB214における各ユーザのユーザ情報との対応関係を一致させるようにしている。

。

- [0082] 配信管理センタ210は、ピースデータdをデジタルコンテンツ再生装置220に送信する前に、ユーザID及びパスワードの確認(即ち、認証)を行う他、プレーヤIDが一致するか否かも含めて確認することから、プレーヤIDは不正使用防止にも役立つことになる。
- [0083] デジタルコンテンツ再生装置220はユーザが使用する汎用のコンピュータである。図中221はCPU等の制御部、222はモニタやスピーカ等の出力部、223はキーボードやマウス等の操作部、224はハードディスク等のメモリ部、225は記録媒体等に対してデータのリード/ライトを行う再生複写部、226は通信を行うための通信部である。
- [0084] メモリ部224にはコンピュータとしてのオペレーションシステム等の基本プログラム以外に図7に示す再生用ソフトウェアが記録されている。この再生用ソフトウェアは配信管理センタ210からユーザ登録を条件として通信回線βを通じてダウンロードされた有償又は無償のソフトウェアであって、コンテンツファイルを再生するのに必要なアプリケーションソフトである。また、メモリ部224には再生用ソフトウェアに割り当てられたプレーヤIDやピースデータdが格納された配信管理センタ210のWEBアドレスの情報が当該再生用ソフトウェアと共に配信管理センタ210から送信され、記録される。更に、メモリ部224には配信管理センタ210から送信されたピースデータd、復号鍵c1、c2等が記録される他、レンタル期間などを示すレンタル情報が記録される。
- 再生用ソフトウェアの内容については後述するが、図7に示す再生用ソフトウェアが制御部221で処理されることより、同コンピュータがデジタルコンテンツ再生装置220としての機能を発揮するようになっている。
- [0085] 以上のように構成されたデジタルコンテンツの不正使用防止システム200の動作について説明し、併せてデジタルコンテンツ再生装置220の動作、配信管理センタ210の動作及び各プログラムの内容について説明する。
- [0086] まず、ユーザが自己のコンピュータ(デジタルコンテンツ再生装置220に相当するコンピュータであり、再生用ソフトウェアがダウンロードされていない状態)の操作部223を操作して通信回線βを介して配信管理センタ210にアクセスし、ユーザ登録の要求を行う。配信管理センタ210は、この要求に応じて図8に示すユーザ登録用割込ブ

ログラムを処理し、ユーザ登録に必要なデータを前記コンピュータに向けて送信する(s21)。その後、ユーザが前記コンピュータの操作部223を通じてユーザ登録用画面が示すところに従って氏名、住所及び支払条件「自己の銀行口座番号又はクレジットカード番号等」等を入力し、この登録データを通信回線 $\beta$ を介して配信管理センタ210に送信する。すると、配信管理センタ210は、これに応じてユーザIDやパスワードを作成し、当該ユーザID等を登録データと共にユーザ情報としてユーザ情報DB214に登録する(

s22) 一方、当該ユーザIDやパスワードを通信回線 $\beta$ を介してユーザのコンピュータに送信する(s23)。そして、ユーザ登録用割込プログラムの処理を終了する。なお、ユーザIDやパスワードはユーザ登録の際にユーザ自身に入力させるようにしても良い。

[0087] その後、ユーザが自己のコンピュータを操作して、配信管理センタ210にアクセスし、再生用ソフトウェアのダウンロードの要求を入力する。この際、ユーザのIDやパスワードが必要になる。すると、ユーザのコンピュータは、その要求を通信回線 $\beta$ を通じて配信管理センタ210に送信する。配信管理センタ210は、この要求に応じて再生用ソフトウェアダウンロード用割込プログラムを処理し、これによりソフトウェアDB215上の再生用ソフトウェア及び復号鍵c1を読み出して通信回線 $\beta$ を介してユーザのコンピュータに送信する。すると、再生用ソフトウェアが同コンピュータのメモリ部224にダウンロードされ、インストールされる。と同時に復号鍵c1がメモリ部224に記録される。これにより同コンピュータがデジタルコンテンツ再生装置220となるのである。

[0088] 次に、コンテンツファイルを取得するに当たり、デジタルコンテンツ再生装置220は、ユーザの操作部223を通じた操作に応じて配信管理センタ210のコンテンツダウンロード用アドレスにアクセスする。すると、配信管理センタ210はコンテンツダウンロード用割込プログラムを処理する。そして、コンテンツファイルリストのデータをデジタルコンテンツ再生装置220に送信する。デジタルコンテンツ再生装置220は、このデータに基づいてコンテンツファイルリストを出力部222に表示出力する。なお、配信管理センタ210にアクセスする際には、再生用ソフトウェアを実行した後、当該ソフトウェアと共に記録されたWEBアドレスに基づいてアクセスしても良いし、ユーザがインタ



ーネットブラウザに登録したWEBアドレスに基いてアクセスしても良い。

[0089] その後、ユーザが操作部223を通じてコンテンツファイルリストからダウンロードするコンテンツファイルを選択する。すると、選択したコンテンツファイルのダウンロードの申込のデータを配信管理センタ210に送信する。

[0090] 配信管理センタ210は、この申込のデータを受信すると、これに含まれるコンテンツIDを参照して当該コンテンツIDに対応するコンテンツファイルをデジタルコンテンツDB211から検索して読み出し、そしてデジタルコンテンツ再生装置220に送信する。デジタルコンテンツ再生装置220は、当該コンテンツファイルを受信すると、メモリ部224のレジストリ又は再生複写部225にセットされた記録媒体に記録する。と同時に、当該コンテンツファイルのファイル名がメモリ部224上の再生用ソフトウェアのプレイリストに記録される。このようにしてコンテンツファイルを取得する。なお、コンテンツファイルのダウンロードについては配信管理センタ210と通信回線 $\beta$ を介して接続された他のコンピュータで取得し、記録媒体に記録しても良い。

[0091] その後、このデジタルコンテンツ再生装置220は、ユーザにより再生用ソフトウェアの実行操作がなされる(コンテンツファイルを記録媒体に記録した場合には再生用ソフトウェアの実行操作がなされる一方で当該記録媒体が再生複写部225にセットされる。)

と、当該再生用ソフトウェアに含まれる再生プレーヤ及びプレイリストのデータを出力部222に表示出力する。すると、再生プレーヤの画面上にプレイリストが表示される(s1)。このプレイリストにはダウンロードしたコンテンツファイルのファイル名と共に、当該コンテンツファイルがレンタル中であるか否かが表示される。即ち、再生の申込がされたことを示す所定のフラグが立っているコンテンツファイルがレンタル中であるとして表示される。そして、このプレイリストに基づき操作部223を通じてレンタル中のコンテンツファイルが再生操作されたか否かを判定する(s2)。

[0092] 再生操作がなされていないと判定すると、操作部223を通じてプレイリストに表示されたレンタル中でないコンテンツファイルの再生の申し込み操作されたか否かを判定する(s3)。その結果、再生の申し込み操作がなされていないと判定すると、操作部2

23を通じて記録媒体の読み込みの操作( DISC LOADの操作)がなされたか否かを判定する(s4)。DISC LOADの操作がなされると、プレイリストに記録されていない記録媒体上の(即ち、他のコンピュータ等で記録媒体上にダウンロードした)

コンテンツファイルを示すコンテンツリストを出力部222に表示出力する(s5)。即ち、メモリ部225上の復号鍵c1を読み出す一方、記録媒体上のコンテンツファイルのヘッダ情報aを読み出し、当該復号鍵c1を用いてヘッダ情報aを復号化し当該ヘッダ情報aに含まれるコンテンツ情報を読み出し、記録媒体上のコンテンツファイルのうち所定のフラグが立っていないコンテンツファイルをコンテンツリストに表示する。

[0093] その後、ユーザによりプレイリスト上のレンタル中でないコンテンツファイル又はコンテンツリスト上のコンテンツファイルの再生の申し込みがなされると( s3又はs6)、メモリ部224上の復号鍵c1を読み出す一方、メモリ部224又は記録媒体上の当該コンテンツファイルのヘッダ情報aを読み出し、当該復号鍵c1を用いてヘッダ情報aを復号化してこれに含まれるコンテンツ情報のWEBアドレスに基き当該ヘッダ情報aに含まれるコンテンツIDを通信回線  $\beta$  を介して配信管理センタ210に送信する。このようにして再生申込処理を行う旨を送信する。

[0094] すると、配信管理センタ210は図9に示すピースデータ配信用割込プログラムを処理し、再生申込処理に必要なデータを通信回線  $\beta$  を介してデジタルコンテンツ再生装置220に送信する( s31)。デジタルコンテンツ再生装置220は、このデータに基づいて再生申込用画面を出力部222に表示出力する(s7)。

[0095] その後、ユーザが再生申込用画面が示すところに従ってレンタル期間を操作部223を通じて順次入力又は選択(これによりレンタル金額が自動的に決まる)し、最後にユーザIDやパスワードをコンテンツファイルの再生申し込みとして操作部223を通じて入力すると(s8)、デジタルコンテンツ再生装置220は、出力部222の表示出力を認証画面に切り換える一方、入力された申し込みデータを通信回線  $\beta$  を介して配信管理センタ210に送信する。この際、メモリ部224又は記録媒体上のコンテンツ情報のコンテンツIDと当該メモリ部224上のプレーヤIDとを読み出し、申し込みデータと一緒に配信管理センタ210に送信する(s9)。

- [0096] すると、配信管理センタ210は、申し込みに係るユーザの認証を確認する(s32)。即ち、送信されたユーザのユーザIDやプレーヤID等を参照してユーザ情報DB214から当該ユーザのユーザ情報を読み出し、当該ユーザが真正のユーザであるか否かを確認する。このとき、配信管理センタ210は、ユーザ情報DB214にレンタル料金の不払い等が所定以上ある不適合者リストが予め用意されており、当該認証と共に不適合者リストに該当する者でないか否かを確認する(なお、不適合者リストの確認は任意である)。
- [0097] 配信管理センタ210は、申し込みに係るユーザが不正なユーザである又は真正のユーザであるものの不適合者リストに該当する者であると確認した場合、ユーザの申し込みを拒否する旨を通信回線βを介してデジタルコンテンツ再生装置220に送信する(s33)。その後、ピースデータ配信用割込プログラムを処理を終了する。
- [0098] 一方、申し込みに係るユーザが真正のユーザであり且つ不適合者リストに該当しない者であることを確認した場合、ユーザのプレーヤID等を参照して当該ユーザのユーザ情報DB214上のユーザ情報に課金を記録する一方、コンテンツIDを参照してピースデータDB216を検索し当該コンテンツIDに対応するピースデータd及び復号鍵c2を読み出し、これを再生の申し込みデータに含まれるレンタル情報と共にユーザの申し込みを承諾する旨の回答として通信回線βを介してデジタルコンテンツ再生装置220に送信する(s34)。その後、ピースデータ配信用割込プログラムを処理を終了する。
- [0099] なお、課金については、所定期間毎にユーザ情報DB214に基き、銀行・カード会社230に請求するか若しくは、ユーザに直接請求し、ユーザに振込やコンビニエンスストア等で支払いをさせるようにする。また、配信管理センタ210が銀行・カード会社230と通信回線βを介して接続されている場合には、即時決済とすることももちろん可能である。
- [0100] デジタルコンテンツ再生装置220は、その後、通信回線βを介してユーザの申し込みを拒否する旨を受信すると(s10)、エラーメッセージを出力部222に表示出力する(s11)。
- [0101] 一方、通信回線βを介してピースデータd、復号鍵c2及びレンタル情報を受信する

と(s10)、所定のフラグを立てる一方、ピースデータd、復号鍵c2及びレンタル情報をメモリ部224に記録する(s12)。と同時に、コンピュータの時計機能を用いてピースデータ送信日時をメモリ部224に記録する。そして、プレイリストを更新して出力部222に表示出力し、当該プレイリスト中にピースデータdを得たコンテンツファイルのファイル名を表示させる(s1)。

- [0102] その後、デジタルコンテンツ再生装置220は、操作部223を通じてプレイリストに基づきレンタル中のコンテンツファイルの再生操作がなされると(s2)、メモリ部224から復号鍵c1を読み出す一方、メモリ部224又は記録媒体上のコンテンツファイルのヘッダ情報aを読み出し、当該復号鍵c1を用いてヘッダ情報aを復号化する。そして、当該ヘッダ情報aに含まれる再生情報を用いてメモリ部224又は記録媒体上のデータ本体bを読み出し、当該データ本体bをメモリ部224上の復号鍵c2で復号化しつつ再生する(s13)。と共に、メモリ部224又は記録媒体上のデータ本体bの開始位置情報を読み出す一方、メモリ部224上のピースデータdを読み出し、開始位置情報からピースデータdに含まれる位置情報までのデータ長や時間のカウントを開始する(s14)。その後、前記カウントが終了したか否かを判定する(s15)。これにより、データ本体bの欠落部分の認識を行う。この判定の結果、カウントが終了したと判定しデータ本体bの欠落部分を認識すると、メモリ部224上のピースデータdを読み出し、当該ピースデータdに含まれる欠落データを当該データ本体bの欠落部分のデータとして読み出しメモリ部224上の復号鍵c2で復号化しつつ再生する(s16)。その後、再びメモリ部224又は記録媒体上のデータ本体bを読み出しメモリ部224上の復号鍵c2で復号化しつつ続きの再生を行う(s17)。なお、この再生用ソフトウェアのプログラムはユーザにより終了の処理が行われることにより終了する。

- [0103] また、再生用ソフトウェアには、上述した基本機能の他、デジタルコンテンツ再生装置220の電源がONにされると、当該デジタルコンテンツ再生装置220に常駐し、ピースデータdの管理を行うピースデータ管理機能を有している。このピースデータ管理機能においては、メモリ部224上のピースデータdの管理を行う一方、ピースデータ送信日時と現在の日時との差をピースデータdが送信された時点からの経過期間として求め、これがレンタル情報に含まれるレンタル期間に達しているときはレンタル期

間外であるとしてメモリ部224上のピースデータd及び復号鍵c2を削除する一方、所定のフラグを倒すようになっている。

[0104] このように不正使用防止システム200においては、ユーザがデジタルコンテンツ再生装置220を使用してコンテンツファイルを再生操作しても、真正の再生の申込者として配信管理センタ210からピースデータdを得ない限り、コンテンツファイルのデータ本体bを再生することができない。よって、コンテンツファイルの一時的な不正使用を防止することができる。しかも、レンタル期間が過ぎたものについては、ピースデータdが削除されるので、二次的な不正使用も防止することができる。さらに、ユーザによりコンテンツファイルが他の記録媒体等にコピーされたとしても、この記録媒体に記録されたコンテンツファイルにはヘッダ情報aに含まれる再生情報が欠落していることから、真正の再生の申込者としてピースデータdを得ない限り、再生することができない。よって、三次的な不正使用も防止することができる。

[0105] しかも、デジタルコンテンツのレンタル期間外においてはメモリ部224上のピースデータd等が自動的に削除されるだけで、コンテンツファイルはそのままである。よって、レンタル期間内外において、デジタルコンテンツ再生装置220の使用してコンテンツファイルを他の記録媒体にコピーすることが可能である。このような記録媒体上のコンテンツファイルを再生するには、デジタルコンテンツ再生装置220を使用して、配信管理センタ210に対する認証及びレンタル使用料の支払いが必要になるので、ここに二次的、三次的使用による課金の回収を確実に行うことが可能になる。

[0106] また、同システムにおいては、上述したようにライト機能を有するコンピュータを使用してコンテンツファイルを記録媒体に簡単に記録することが可能であるので、レンタルビデオ店等ではビデオテープやCD、DVD等の記録媒体を陳列する代わりに当該コンピュータを設置する形態を取ることができる。このようにすれば、前記記録媒体の返却は不要であるから、店側及び顧客の双方にメリットがある。しかも、顧客に関しては、どのようなコンテンツファイルをダウンロードしたか店員に知られることがないので、デジタルコンテンツの種類によっては借り易くなる。この場合、レンタルビデオ店としての形態を取る必要はなく、インターネットカフェの一サービスとして提供するようにすることが可能であることは言うまでもない。なお、レンタルビデオ店やインターネット

カフェにコンテンツDBを設置するようにしても良い。

[0107] この不正使用防止システム200については、ヘッダ情報とデータ本体とを有したコンテンツファイルが当該データ本体の一部を欠落させた状態で記録された第1のデータベースと、この欠落データ及び当該欠落データがデータ本体のどの部分であるかを示す位置情報が記録された第2のデータベースとを有するサーバであって当該コンテンツファイルを通信回線を介して配信可能である一方、当該コンテンツファイルの利用を管理する配信管理手段と、この配信管理手段との間で通信回線を介して通信可能であり且つ配信管理手段から配信されたコンテンツファイルを再生する際に使用されるデジタルコンテンツ再生装置とを備え、ユーザによりコンテンツファイルのダウンロードの要求がデジタルコンテンツ再生装置に入力されると、デジタルコンテンツ再生装置が当該要求を通信回線を介して配信管理手段に送信し、配信管理手段が当該要求に係るコンテンツファイルを通信回線を介してデジタルコンテンツ再生装置に送信し、デジタルコンテンツ再生装置が当該コンテンツファイルを受信してメモリ部又は記録媒体に記録する一方、ユーザによりコンテンツファイルの再生の申し込みがデジタルコンテンツ再生装置に入力されると、デジタルコンテンツ再生装置が当該申し込みを通信回線を介して配信管理手段に送信し、配信管理手段が当該申し込みに係るコンテンツファイルの欠落データ及びその位置情報を通信回線を介してデジタルコンテンツ再生装置に同時又は相前後して送信し、デジタルコンテンツ再生装置は当該欠落データ及びその位置情報を同時又は相前後して受信してメモリ部に記録し、メモリ部又は記録媒体上のコンテンツファイルのデータ本体を読み出して再生すると共に、メモリ部から読み出した位置情報を参照して前記データ本体の欠落部分を認識し、メモリ部上の欠落データを当該欠落部分のデータとして読み出して再生する構成となっている限りどのような設計変形を行ってもかまわない。

[0108] よって、配信管理センタ210は、デジタルコンテンツDB211が一つであるとしたが、複数であっても良い。この場合、例えば一のDBに映画のコンテンツファイルを、二のDBに音楽のコンテンツファイルをといったように異なる種類のコンテンツファイル群をDBにそれぞれ格納するようにしても良いし、各DBに格納するコンテンツファイル群を同じとし混雑時に一のDBにアクセスが集中するのを防ぐようにしても良い。同様の

ことがピースデータDB216にも言える。また、配信管理センタ210はデジタルコンテンツDB211、ピースデータDB216を有するとしたが、デジタルコンテンツDB211、ピースデータDB216を配信管理センタ210とは別の場所に設置することも可能である。この場合、配信管理センタ210はユーザの認証をした上でデジタルコンテンツDB211、ピースデータDB216のWEBアドレスをデジタルコンテンツ再生装置220に送信し、デジタルコンテンツ再生装置220は当該WEBアドレスに基づいてデジタルコンテンツDB211、ピースデータDB216にアクセスし、コンテンツファイル、ピースデータdを得るようにすれば良い。

[0109] また、デジタルコンテンツDB211には、ヘッダ情報a及びデータ本体bが各々暗号化された状態で記録されているとしたが、暗号化するか否かは任意である。ただ、少なくともデータ本体bが暗号化されていることが望ましい。また、コンテンツファイルはヘッダ情報a及びデータ本体bとを有する構成であるとしたが、その他の情報を付加した状態で記録することは勿論可能である。その他の情報としては、ユーザのコンピュータに再生用ソフトウェアがインストールされているか否かを判断して、インストールされていないと判断した場合には、配信管理センタ210のHPに自動的にアクセスするプログラム等がある。このプログラムを記録させておくと、ユーザが自己のコンピュータ（デジタルコンテンツ再生装置220に相当するコンピュータであり、再生用ソフトウェアがダウンロードされていない状態）に予め入手したコンテンツファイルを実行しようとする、配信管理センタ210のWEBアドレスを読み出し、これに基づいて配信管理センタ210に自動的にアクセスする。その後、上述した手順で再生用ソフトウェアを入手するようにすることができる。なお、コンテンツファイルについては、一部が欠落しているとしたが、複数箇所を欠落させることも当然可能であることは言うまでもない。

[0110] 位置情報については、開始位置情報から欠落部分までのデータ長や時間であるとしたが、欠落部分を示すアドレス値等であっても良い。この場合、次に読み出すべき流通用記録媒体 $\alpha$ 上のデータ本体bのアドレス値と位置情報とが一致するか否かを逐次判定し、この判定の結果、一致しないと判定したときには前記アドレス値の示すメモリ部224又は記録媒体上のデータ本体bを読み出し、一致すると判定したときにはメモリ部224上の欠落データを読み出すようにする。

- [0111] ピースデータdについては、欠落データとその位置情報とからなるとしたが、前記位置情報を含めるか否かは任意である。この場合、例えば、予めデータ本体bの欠落部分の前に欠落部分であることを示す欠落位置情報を記録しておき、データ本体bを再生すると共に、開始位置情報から欠落位置情報までをカウントし、このカウントが終了すると、メモリ部224上の欠落データを当該欠落部分のデータとして再生するようにすれば良い。或いは、予めデータ本体bの欠落部分の位置を決定しておくと共に、再生用ソフトウェアに欠落データの位置情報が予め用意しておく。そして、データ本体bを再生すると共に、この位置情報に基づいてデータ本体bの欠落部分を認識し、メモリ部224上の欠落データを当該欠落部分のデータとして再生するようにすることもできる。
- [0112] このように再生用ソフトウェアの内容については、一例に過ぎず、同様の内容を実現可能である限りどのような設計変形を行ってもかまわない。ユーザ登録用割込プログラム、再生用ソフトウェアダウンロード用割込プログラム及びピースデータ配信用割込プログラムについても同様である。
- [0113] また、コンテンツファイルをデジタルコンテンツ再生装置220のメモリ部224に記録した場合には、レンタル期間が過ぎると、ピースデータdと共に、コンテンツファイルを削除するようにしても良いし、ピースデータdとは別に、コンテンツファイルを受信した時点からの経過期間を求め、当該経過期間が所定期間に達したときは、当該コンテンツファイルを削除するようにしても良い。
- [0114] なお、第2の実施の形態については、レンタルではなく有償又は無償で配信されたコンテンツファイルの不正使用を防止するシステムに設計変更することも可能であり、この場合であっても上記と同様のメリットを奏する。この場合に使用される再生用ソフトウェアについては、配信されたコンテンツファイルがレンタル期間外であるときの処理を削除するだけの内容で良い。また、デジタルコンテンツ再生装置220に関しては、再生用ソフトウェアを配信管理センタ210からダウンロードするのではなく、CD等を記録媒体を通じてインストールするようにしても良い。また、コンピュータではなく専用装置の形態にすることもできるのは当然である。

### 実施例 3



- [0115] 次に、本発明の第3の実施の形態を図面を参照しながら説明する。図10は本発明の第3の実施の形態に係るデジタルコンテンツの不正使用防止システムの構成図、図11はデジタルコンテンツの不正使用防止システムに使用される再生用ソフトウェアのフローチャート、図12はコンテンツダウンロード用割込プログラムのフローチャートである。
- [0116] 図10に示すデジタルコンテンツの不正使用防止システム300は不正使用防止システム200と同じ構成である。異なる点は、デジタルコンテンツ再生装置320のメモリ部324に記録される再生用ソフトウェアの内容(図11参照)と、配信管理センタ310のメモリ部317に記録されたコンテンツダウンロード用割込プログラムの内容(図12参照)とである。以下、その相違点について詳しく説明し、重複する部分については説明を省略する。
- [0117] デジタルコンテンツ再生装置320には、実施例2と同様の手順で再生用ソフトウェアがダウンロードされ、メモリ部324に記録されている。
- [0118] その後、コンテンツファイルを取得するに当たり、デジタルコンテンツ再生装置320は、ユーザの操作部323を通じた操作に応じて配信管理センタ310のコンテンツダウンロード用のアドレスにアクセスする。すると、配信管理センタ310は、図12に示すコンテンツダウンロード用割込プログラムを処理する。そして、レンタル申込処理に必要なコンテンツファイルリスト等のデータを通信回線 $\beta$ を介してデジタルコンテンツ再生装置320に送信する(s21)。デジタルコンテンツ再生装置320は、このデータに基づいてレンタル申込用画面を出力部322に表示出力する。
- [0119] その後、ユーザがレンタル申込用画面が示すところに従ってレンタルするコンテンツファイル及びそのレンタル期間を操作部323を通じて順次入力又は選択(これによりレンタル金額が自動的に決まる)し、最後にユーザIDやパスワードをコンテンツファイルのレンタル申し込みとして操作部323を通じて入力すると、デジタルコンテンツ再生装置320は、出力部322の表示出力を認証画面に切り換える一方、入力された申し込みデータを通信回線 $\beta$ を介して配信管理センタ310に送信する。この際、メモリ部324上のプレーヤIDを読み出し、申し込みデータと一緒に配信管理センタ210に送信する。

- [0120] すると、配信管理センタ310は、申し込みに係るユーザの認証を確認する(22)。即ち、送信されたユーザのユーザIDやプレーヤID等を参照してユーザ情報DB314から当該ユーザのユーザ情報を読み出し、当該ユーザが真正のユーザであるか否かを確認する。このとき、配信管理センタ310は、ユーザ情報DB314にレンタル料金の不払い等が所定以上ある不適合者リストが予め用意されており、当該認証と共に不適合者リストに該当する者でないか否かを確認する(なお、不適合者リストの確認は任意である)。
- [0121] 配信管理センタ310は、申し込みに係るユーザが不正なユーザである又は真正のユーザであるものの不適合者リストに該当する者であると確認した場合、ユーザの申し込みを拒否する旨を通信回線 $\beta$ を介してデジタルコンテンツ再生装置320に送信する(s23)。
- [0122] 一方、申し込みに係るユーザが真正のユーザであり且つ不適合者リストに該当しない者であることを確認した場合、選択されたコンテンツファイルをそのコンテンツIDを参照してデジタルコンテンツDB311から検索して読み出す一方、当該コンテンツIDに対応するピースデータd及び復号鍵c2をピースデータDB316から検索して読み出し、そしてコンテンツファイル、ピースデータd及び復号鍵c2をレンタル情報と共にユーザの申し込みを承諾する旨の回答として通信回線 $\beta$ を介して順次デジタルコンテンツ再生装置320に送信する(s24)。そして、ユーザのプレーヤID等を参照して当該ユーザのユーザ情報DB314上のユーザ情報に課金を記録する。
- [0123] なお、課金については、所定期間毎にユーザ情報DB314に基いて集計し、銀行・カード会社330に請求するか若しくは、ユーザに直接請求し、ユーザに振込やコンビニエンスストア等で支払いをさせるようにする。また、配信管理センタ310が銀行・カード会社330と通信回線 $\beta$ を介して接続されている場合には、即時決済とすることももちろん可能である。
- [0124] デジタルコンテンツ再生装置320は、その後、通信回線 $\beta$ を介してユーザの申し込みを拒否する旨を受信すると、エラーメッセージを出力部322に表示出力する。
- [0125] 一方、当該コンテンツファイル等を受信すると、当該コンテンツファイルをメモリ部324のレジストリ又は複写部325にセットされた記録媒体に記録する一方、当該ピース

データd、復号鍵c2及びレンタル情報を予め決められたメモリ部324のコンテンツファイルが記録されるレジストリとは別のピースデータ用のレジストリに記録する。と同時に、当該コンテンツファイルのファイル名がメモリ部324上の再生用ソフトウェアのプレイリストに記録される。そして、所定のフラグを立てる。

[0126] その後、ユーザにより再生用ソフトウェアの実行操作がなされる(コンテンツファイルを記録媒体に記録した場合には再生用ソフトウェアの実行操作がなされる一方で当該記録媒体がセットされる。)と、当該再生用ソフトウェアに含まれる再生プレーヤ及びプレイリストのデータを出力部322に表示出力する。すると、再生用ソフトウェアの画面上にプレイリストが表示される(s1)。このプレイリストにはコンテンツファイルのファイル名と共に、当該コンテンツファイルがレンタル中である旨が表示される。即ち、所定のフラグが立っているコンテンツファイルがレンタル中であるとして表示される。そして、このプレイリストに基づき操作部323を通じてレンタル中のコンテンツファイルが再生操作されたか否かを判定する(s2)。

[0127] 再生操作がなされていないと判定すると、前記プレイリストに基づき操作部323を通じてレンタル中でないコンテンツファイルの再生の申し込みがされたか否かを判定する(s3)。即ち、レンタル期間が終了したコンテンツファイルの再レンタルの申し込みがされたか否かを判定する。その結果、再生の申し込みがなされたと判定すると、メモリ部324上の復号鍵c1を読み出す一方、メモリ部324又は記録媒体上の当該コンテンツファイルのヘッダ情報aを読み出し、当該復号鍵c1を用いてヘッダ情報aを復号化して当該ヘッダ情報aに含まれるコンテンツ情報のWEBアドレスに基きコンテンツIDを通信回線βを介して再生申込処理を行う旨として配信管理センタ310に送信する。

[0128] すると、配信管理センタ310はピースデータ配信用割込プログラムを処理する(図9参照)。そして、再生申込処理に必要なデータを通信回線βを介してデジタルコンテンツ再生装置320に送信する(s31)。デジタルコンテンツ再生装置320は、このデータに基づいて再生申込用画面を出力部322に表示出力する(s4)。

[0129] その後、ユーザが再生申込用画面が示すところに従ってレンタル期間を操作部32

3を通じて順次入力又は選択(これによりレンタル金額が自動的に決まる)し、最後にユーザIDやパスワードをコンテンツファイルの再生申し込みとして操作部323を通じて入力すると(s5)、デジタルコンテンツ再生装置320は、出力部322の表示出力を認証画面に切り換える一方、入力された申し込みデータを通信回線 $\beta$ を介して配信管理センタ310に送信する。この際、メモリ部324又は記録媒体上のコンテンツ情報のコンテンツIDと当該メモリ部324上のプレーヤIDとを読み出し、申し込みデータと一緒に配信管理センタ310に送信する(s6)。

[0130] すると、配信管理センタ310は、申し込みに係るユーザの認証を確認する(s32)。即ち、送信されたユーザのユーザIDやプレーヤID等を参照してユーザ情報DB314から当該ユーザのユーザ情報を読み出し、当該ユーザが真正のユーザであるか否かを確認する。このとき、配信管理センタ310は、ユーザ情報DB314にレンタル料金の不払い等が所定以上ある不適当者リストが予め用意されており、当該認証と共に不適当者リストに該当する者でないか否かを確認する(なお、不適当者リストの確認は任意である)。

[0131] 配信管理センタ310は、申し込みに係るユーザが不正なユーザである又は真正のユーザであるものの不適当者リストに該当する者であると確認した場合、ユーザの申し込みを拒否する旨を通信回線 $\beta$ を介してデジタルコンテンツ再生装置320に送信する(s33)。そして、ピースデータ配信用割込プログラムの処理を終了する。

[0132] 一方、申し込みに係るユーザが真正のユーザであり且つ不適当者リストに該当しない者であることを確認した場合、ユーザのプレーヤID等を参照して当該ユーザのユーザ情報DB314上のユーザ情報に課金を記録する一方、ピースデータDB316を検索して上記コンテンツIDに対応するピースデータd及び復号鍵c2を読み出し、これを再生の申し込みデータに含まれるレンタル情報と共にユーザの申し込みを承諾する旨の回答として通信回線 $\beta$ を介してデジタルコンテンツ再生装置320に送信する(s34)。そして、ピースデータ配信用割込プログラムの処理を終了する。なお、課金については上記と同様に行う。

[0133] デジタルコンテンツ再生装置320は、その後、通信回線 $\beta$ を介してユーザの申し込みを拒否する旨を受信すると(s7)、エラーメッセージを出力部322に表示出力する(

s8)。

[0134] 一方、配信管理センタ310からユーザの申し込みを承諾する旨の回答としてピースデータd、復号鍵c2及びレンタル情報が通信回線 $\beta$ を介して送信されると(a7)、所定のフラグを立てる一方、ピースデータd、復号鍵c2及びレンタル情報を上述したメモリ部324のピースデータ用のレジストリに記録する(s9)。と同時に、コンピュータの時計機能を用いてピースデータ送信日時をメモリ部324に記録する。そして、プレイリストを更新してピースデータdを取得したコンテンツファイルがレンタル中であるとして出力部322に表示出力する(s1)。

[0135] その後、デジタルコンテンツ再生装置320は、操作部323を通じてプレイリストに基づきレンタル中のコンテンツファイルの再生操作がなされると(s2)、メモリ部324から復号鍵c1を読み出す一方、メモリ部324又は記録媒体上のコンテンツファイルのヘッダ情報aを読み出し、当該復号鍵c1を用いてヘッダ情報aを復号化する。そして、当該ヘッダ情報aに含まれる再生情報を用いてメモリ部324又は記録媒体上のデータ本体bを読み出し、当該データ本体bをメモリ部324上の復号鍵c2で復号化しつつ再生する(s10)。と共に、メモリ部324又は記録媒体上のデータ本体bの開始位置情報を読み出す一方、メモリ部324上のピースデータdを読み出し、開始位置情報からピースデータdに含まれる位置情報までのデータ長や時間のカウントを開始する(s11)。その後、前記カウントが終了したか否かを判定する(s12)これにより、データ本体bの欠落部分の認識を行う。この判定の結果、カウントが終了したと判定しデータ本体bの欠落部分を認識すると、メモリ部324上のピースデータdを読み出し、当該ピースデータdに含まれる欠落データを当該データ本体bの欠落部分のデータとして読み出しメモリ部324上の復号鍵c2で復号化しつつ再生する(s13)。その後、再びメモリ部324又は記録媒体上のデータ本体bを読み出しメモリ部324上の復号鍵c2で復号化しつつ続きの再生を行う(s14)。なお、この再生用ソフトウェアのプログラムはユーザにより終了の処理が行われることにより終了する。

[0136] また、再生用ソフトウェアには、上述した基本機能の他、デジタルコンテンツ再生装置320の電源がONにされると、当該デジタルコンテンツ再生装置320に常駐し、ピースデータdの管理を行うピースデータ管理機能を有している。このピースデータ管

理機能においては、メモリ部324上のピースデータdの管理を行う一方、ピースデータ送信日時と現在の日時との差をピースデータdが送信された時点からの経過期間として求め、これがレンタル情報に含まれるレンタル期間に達しているときはレンタル期間外であるとしてメモリ部324上のピースデータd及び復号鍵c2を削除する一方、所定のフラグを倒すようになっている。

[0137] このような不正使用防止システム300においては、コンテンツファイルと同時にそのピースデータdを得ることができるので、実施例2と比べてコンテンツファイルの真正な一時的使用が容易になる。また、レンタル期間が過ぎたものについては、ピースデータdが削除されるので、二次的な不正使用を防止することができる。しかも、ユーザによりコンテンツファイルが記録媒体に記録されたとしても、この記録媒体に記録されたコンテンツファイルにはヘッダ情報aに含まれる再生情報が欠落していることから、真正の再生の申込者としてピースデータdを得ない限り、再生することができない。よって、三次的な不正使用も防止することができる。

[0138] また、デジタルコンテンツのレンタル期間外においてはメモリ部324上のピースデータd等が自動的に削除されるだけで、コンテンツファイルはそのままである。よって、レンタル期間外において、デジタルコンテンツ再生装置320の使用してコンテンツファイルを他の記録媒体にコピーすることが可能である。このような記録媒体上のコンテンツファイルを再生するには、デジタルコンテンツ再生装置320を使用して、配信管理センタ310に対する認証及びレンタル使用料の支払いが必要になるので、ここに二次的、三次的使用による課金の回収を確実に行うことが可能になる。

[0139] 配信管理センタ310は、デジタルコンテンツDB311が一つであるとしたが、複数であっても良い。この場合、例えば1のDBに映画のコンテンツファイルを、2のDBに音楽のコンテンツファイルをといったように異なる種類のコンテンツファイル群をDBにそれぞれ格納するようにしても良いし、各DBに格納するコンテンツファイル群を同じとし混雑時に一のDBにアクセスが集中するのを防ぐようにしても良い。同様のことがピースデータDB316にも言える。また、配信管理センタ310はデジタルコンテンツDB311、ピースデータDB316を有するとしたが、デジタルコンテンツDB311、ピースデータDB316を配信管理センタ310とは別の場所に設置することも可能である。この場

合、配信管理センタ310はユーザの認証をした上でデジタルコンテンツDB311、ピースデータDB316のWEBアドレスをデジタルコンテンツ再生装置320に送信し、デジタルコンテンツ再生装置320は当該WEBアドレスに基づいてデジタルコンテンツDB311、ピースデータDB316にアクセスし、コンテンツファイル、ピースデータdを得るようにすれば良い。

[0140] また、デジタルコンテンツDB311には、ヘッダ情報a及びデータ本体bが各々暗号化された状態で記録されているとしたが、暗号化するか否かは任意である。ただ、少なくともデータ本体bが暗号化されていることが望ましい。

[0141] また、コンテンツファイルはヘッダ情報a及びデータ本体bとを有する構成であるとしたが、その他の情報を付加した状態で記録することは勿論可能である。その他の情報としては、ユーザのコンピュータに再生用ソフトウェアがインストールされているか否かを判断して、インストールされていないと判断した場合には、配信管理センタ310のHPに自動的にアクセスするプログラム等がある。このプログラムを記録させておくと、ユーザが自己のコンピュータ(デジタルコンテンツ再生装置320に相当するコンピュータであり、再生用ソフトウェアがダウンロードされていない状態)に予め入手したコンテンツファイルを実行しようとする、配信管理センタ310のWEBアドレスを読み出し、これに基づいて配信管理センタ310に自動的にアクセスする。その後、上述した手順で再生用ソフトウェアを入手することができる。なお、コンテンツファイルについては、一部が欠落しているとしたが、複数箇所を欠落させることも当然可能であることは言うまでもない。

[0142] 位置情報については、開始位置情報から欠落部分までのデータ長や時間であるとしたが、欠落部分を示すアドレス値等であっても良い。この場合、次に読み出すべき流通用記録媒体 $\alpha$ 上のデータ本体bのアドレス値と位置情報とが一致するか否かを逐次判定し、この判定の結果、一致しないと判定したときには前記アドレス値の示すメモリ部324又は記録媒体上のデータ本体bを読み出し、一致すると判定したときにはメモリ部324上の欠落データを読み出すようにする。

[0143] ピースデータdについては、欠落データとその位置情報とからなるとしたが、前記位置情報を含めるか否かは任意である。この場合、例えば、予めデータ本体bの欠落部

分の前に欠落部分であることを示す欠落位置情報を記録しておき、データ本体bを再生すると共に、開始位置情報から欠落位置情報までをカウントし、このカウントが終了すると、メモリ部324上の欠落データを当該欠落部分のデータとして再生するようにすれば良い。或いは、予めデータ本体bの欠落部分の位置を決定しておくと共に、再生用ソフトウェアに欠落させた欠落データの位置情報が予め用意しておく。そして、データ本体bを再生すると共に、この位置情報に基づいてデータ本体bの欠落部分を認識し、メモリ部324上の欠落データを当該欠落部分のデータとして再生するようにすることもできる。

- [0144] このように再生用ソフトウェアの内容については、一例に過ぎず、同様の内容を実現可能である限りどのような設計変形を行ってもかまわない。また、コンテンツファイルダウンロード用割込プログラムの内容については、コンテンツファイルのダウンロードの申し込みによりピースデータdをコンテンツファイルと共に又は別にダウンロードする内容となっている限りどのような設計変形を行ってもかまわない。ユーザ登録用割込プログラム、再生用ソフトウェアダウンロード用割込プログラム及びピースデータ配信用割込プログラムについても同様である。
- [0145] また、コンテンツファイルをデジタルコンテンツ再生装置320のメモリ部324に記録した場合には、レンタル期間が過ぎると、ピースデータdと共に、コンテンツファイルを削除するようにしても良し、ピースデータdとは別に、コンテンツファイルを受信した時点からの経過期間を求め、当該経過期間が所定期間に達したときは、当該コンテンツファイルを削除するようにしても良い。
- [0146] なお、第3の実施の形態については、レンタルではなく有償又は無償で配信されたコンテンツファイルの不正使用を防止するシステムに設計変更することも可能であり、この場合であっても上記と同様のメリットを奏する。この場合に使用される再生用ソフトウェアについては、配信されたコンテンツファイルがレンタル期間外であるときの処理を削除するだけの内容で良い。また、デジタルコンテンツ再生装置320に関しては、再生用ソフトウェアを配信管理センタ310からダウンロードするのではなく、CD等の記録媒体を通じてダウンロードするようにしても良い。また、コンピュータではなく専用装置の形態にすることもできるのは当然である。



#### 実施例 4

- [0147] 次に、本発明の第4の実施の形態を図面を参照しながら説明する。図13は本発明の第4の実施の形態に係るデジタルコンテンツの不正使用防止システムの構成図、図14は同システムに使用される再生用ソフトウェアのフローチャート、図15は同システムのコンテンツファイルを示す図であって、(a)がデータ本体のイメージ図、(b)がデータ本体の $\alpha$ 部分のイメージ図、図16は同システムに用いられる流通用記録媒体作成装置であるコンピュータにより実行される記録媒体作成用ソフトウェアのフローチャートである。
- [0148] 図13に示すデジタルコンテンツの不正使用防止システム400は不正使用防止システム100と同じ構成である。異なる点は、流通用記録媒体 $\alpha$ に記録されたコンテンツファイルの構成、デジタルコンテンツ再生装置420の補助記憶部425に記録される再生用ソフトウェアの内容(図14参照)である。以下、その相違点について詳しく説明し、重複する部分については説明を省略する。
- [0149] デジタルコンテンツ再生装置420はユーザが使用する汎用のコンピュータである。図中421はCPU等の制御部、422はモニタやスピーカ等の出力部、423はキーボードやマウス等の操作部、424は流通用記録媒体 $\alpha$ 等に対してデータのリード/ライトを行う再生複写部、425はハードディスク等の補助記憶部、426はDRAM等の主記憶部、427は通信回線 $\beta$ に接続される通信を行うための通信部である。
- [0150] 補助記憶部425にはコンピュータとしてのオペレーションシステム等の基本プログラム以外に、図14に示す再生用ソフトウェアが記録されている。再生用ソフトウェアの内容については後述するが、同ソフトウェアが主記憶部426上で制御部421に処理されることより、流通用記録媒体 $\alpha$ に記録されたデータ本体bを主記憶部426に復号化ビット長毎に順次転送させ、主記憶部426上の当該データを復号化ビット長毎に順次復号化させ、当該データを圧縮状態から元の状態に戻して再生(リード)するデジタルコンテンツ再生装置420としての機能を発揮するようになっている。
- [0151] 流通用記録媒体 $\alpha$ 上のコンテンツファイルは、ヘッダ情報aと、MPEG等の圧縮方式で圧縮され、周知の暗号化がされ、当該データ本体bの一部が欠落され、当該欠落部分をに詰めて連続させ、その後端に欠落させた部分と同じビット長のダミーデー

タが付加されたデータ本体b(図15参照)とを有する。この流通用記録媒体 $\alpha$ は実施例1の流通用記録媒体作成装置140の制御部142がメモリ部145上の図16に示すプログラムを処理することにより作成される。まず、入力部141にセットされたマスターディスクからコンテンツファイルのヘッダ情報aを読み出し、当該ヘッダ情報aに含まれる再生情報のみを暗号化し、当該ヘッダ情報aを記録部143にセットされたDVD等の記録媒体に記録する(s1)。次に、マスターディスクからコンテンツファイルのデータ本体bを読み出し(s2)、圧縮し(s3)、暗号化する(s4)。その後、当該データ本体bの一部を分離する(s5)。データ本体bを複数箇所分離する場合には、主記憶部426に転送される復号化ビット長のデータを1ブロックとして当該1ブロックのデータからその一部を分離する(s5)。そして、分離した当該欠落データをその位置情報と共にピースデータdとしてピースデータ用メモリ144に記録する(s6)。一方、当該データ本体bの欠落部分を詰めて当該データ本体bを連続させる(s7)と共に、欠落させた部分と同じビット長のダミーデータをメモリ部145から読み出して当該データ本体bの後端に付加する(s8)。データ本体bを複数箇所欠落させた場合には、欠落データのビット長×欠落箇所数のビット長を有するダミーデータデータ本体bの後端に付加する(s8)。そして、当該データ本体bを記録部143にセットされたDVD等の記録媒体に記録する(s9)。これで同ソフトウェアの処理が終了となる。なお、データ本体bを複数箇所分離する場合も復号化ビット長のデータを1ブロックとすることなく分離させることが可能である。

- [0152] 欠落データのビット長は、復号化ビット長と異なるビット長であり、且つ当該復号化ビット長の約数と異なるビット長とする。データ本体bを複数箇所欠落させる場合には、欠落データのビット長×欠落箇所数が復号化ビット長の約数と異なるビット長とする。例えば、復号化ビット長を10バイト(即ち、80ビット)としたとき、欠落データのビット長を10バイト及びその約数以外のバイト数のビット長である7バイト(即ち、56ビット)、13バイト(即ち、104ビット)等とする。欠落データのビット長を7バイトとした場合、データ本体bを10、20箇所欠落させないようにする。なぜなら、復号化ビット長が10バイトあるときに、欠落データのビット長を20バイトとすると、欠落部分以降の復号化ビット長のデータのデータ列が欠落データを欠落させる前と欠落させた後とで同じになり、

その結果、欠落部分以降のデータ本体bが再生可能となるからである。また、ビット長が7バイトである欠落データを10箇所欠落させると、データ本体bの10箇所目の欠落部分以降の復号化ビット長のデータ列が欠落データを欠落させる前と欠落させた後とで同じになり、その結果、10箇所目の欠落部分以降のデータ本体bが再生される可能性が生じるからである。

- [0153] 以上のように構成されたデジタルコンテンツの不正使用防止システム400のデジタルコンテンツ再生装置420を用いたデジタルコンテンツの不正使用防止方法を説明すると共に、管理センタ410の動作、デジタルコンテンツ再生装置420の動作及び各プログラムの内容について説明する。暗号鍵c1、c2は管理センタ410のピースデータDB441に記録されているものとする。以下、説明の便宜上、データ本体bは一箇所のみ欠落しているものとして説明する。
- [0154] まず、デジタルコンテンツ再生装置420には、実施例1と同様の手順で再生用ソフトウェアがダウンロードされ、補助記憶部425に記録されている。
- [0155] このデジタルコンテンツ再生装置420は、ユーザにより流通用記録媒体 $\alpha$ が再生複写部424にセットされる一方、再生用ソフトウェアが実行操作されると、当該再生用ソフトウェアを補助記憶部425から主記憶部426に読み出して処理し、当該再生用ソフトウェアに含まれる再生プレーヤ、プレイリスト等のデータを主記憶部426上に読み出し、出力部422に表示出力する。すると、当該再生プレーヤの画面上にレンタル中のコンテンツを示すプレイリストが表示される(s1)。即ち、再生の申込がされたことを示す所定のフラグが立っているコンテンツファイルのファイル名がプレイリストに表示される。そして、このプレイリストに基づき操作部423を通じて再生操作がなされたか否かを判定する(s2)。
- [0156] 再生操作がなされていないと判定すると、操作部423を通じて流通用記録媒体 $\alpha$ の読み込みの操作(DISC LOADの操作)がなされたか否かを判定する(s3)。DISC LOADの操作がなされると、再生の申し込みがされていないコンテンツファイルを示すコンテンツリストを主記憶部426上に読み出し、出力部422に表示出力する(s4)。即ち、流通用記録媒体 $\alpha$ 上のコンテンツファイルのうち所定のフラグが立っていないコンテンツファイルのヘッダ情報aに含まれるコンテンツ情報を主記憶部426上

に読み出し、コンテンツリストに表示する。

- [0157] その後、ユーザによりコンテンツリスト上のコンテンツファイルの再生の申し込み操作がなされると、流通用記録媒体  $\alpha$  上の当該コンテンツファイルのヘッダ情報aに含まれるコンテンツ情報を主記憶部426上に読み出す。そして、当該コンテンツ情報に含まれるWEBアドレスに基づき当該コンテンツ情報に含まれるコンテンツIDを通信回線  $\beta$  を介して管理センタ410に送信する。このようにして再生申込処理を行う旨を送信する。
- [0158] すると、管理センタ410はピースデータ配信用割込プログラムを処理する(図4を借りて参照)。そして、メモリ部416から再生申込処理に必要なデータを読み出し、通信回線  $\beta$  を介してデジタルコンテンツ再生装置420に送信する(s31)。デジタルコンテンツ再生装置420は、このデータに基づいて再生申込用画面のデータを主記憶部426上に読み出し、出力部422に表示出力する(s5)。
- [0159] その後、ユーザが再生申込用画面が示すところに従ってレンタル期間を操作部423を通じて順次入力又は選択(これによりレンタル金額が決まる)し、最後にユーザIDやパスワードを流通用記録媒体  $\alpha$  の再生申し込みとして操作部423を通じて入力すると(s6)、デジタルコンテンツ再生装置420は、入力された申し込みデータを通信回線  $\beta$  を介して管理センタ410に送信する。この際、流通用記録媒体  $\alpha$  上のヘッダ情報aのコンテンツ情報に含まれるコンテンツID及び補助記憶部425上のプレーヤIDを主記憶部426上に読み出し、申し込みデータと一緒に管理センタ410に送信する(s7)。
- [0160] すると、管理センタ410は、当該記申し込みデータ等を受信すると、当該申し込みに係るユーザの認証を確認する(s32)。即ち、受信したユーザのユーザIDやプレーヤID等を参照してユーザ情報DB414から当該ユーザのユーザ情報を読み出し、当該ユーザが真正のユーザであるか否かを確認する。このとき、管理センタ410は、ユーザ情報DB414にレンタル料金の不払い等が所定以上ある不適当者リストが予め用意されており、当該認証と共に不適当者リストに該当する者でないか否かを確認する(この不適当者リストの確認は任意である)。

- [0161] 管理センタ410は、申し込みに係るユーザが不正なユーザである又は真正のユーザであるものの不適合者リストに該当する者であると確認した場合、ユーザの申し込みを拒否する旨を通信回線 $\beta$ を介してデジタルコンテンツ再生装置420に送信する(s33)。そして、ピースデータ配信用割込プログラムを処理を終了する。
- [0162] 一方、申し込みに係るユーザが真正のユーザであり且つ不適合者リストに該当しない者であることを確認した場合、ユーザのプレーヤID等を参照して当該ユーザのユーザ情報DB414上のユーザ情報に課金を記録する一方、コンテンツIDを参照してピースデータDB111を検索し当該コンテンツIDに対応する復号鍵c1、c2及びピースデータdを読み出し、これを申し込みデータに含まれるレンタル期間等を示すレンタル情報と共にユーザの申し込みを承諾する旨の回答として通信回線 $\beta$ を介してデジタルコンテンツ再生装置420に送信する(s34)。そして、ピースデータ配信用割込プログラムを処理を終了する。
- [0163] なお、課金については、所定期間毎にユーザ情報DB414に基いて集計し、銀行・カード会社430に請求するか若しくは、ユーザに直接請求してユーザに振込やコンビニエンスストア等で支払いをさせるようにする。また、管理センタ410が銀行・カード会社130と通信回線 $\beta$ を介して接続されている場合には、即時決済とすることももちろん可能である。
- [0164] デジタルコンテンツ再生装置420は、その後、通信回線 $\beta$ を介してユーザの申し込みを拒否する旨を受信すると(s8)、拒否する旨のデータに含まれるエラーメッセージのデータを出力部422に表示出力する(s9)。一方、通信回線 $\beta$ を介して復号鍵c1、c2、ピースデータd及びレンタル情報を受信すると(a8)、所定のフラグをセットする一方、復号鍵c1、c2、ピースデータd及びレンタル情報を補助記憶部425に記録する(s10)。と同時に、コンピュータの時計機能を用いてピースデータ送信日時を補助記憶部425に記録する。そして、プレイリストを主記憶部426上に読み出して更新し、出力部422に表示出力する(s1)。これにより、当該プレイリスト中にピースデータdを得たコンテンツファイルのファイル名が表示される。
- [0165] その後、デジタルコンテンツ再生装置420は、操作部423を通じてプレイリストに基づきコンテンツファイルの再生操作がなされると(s2)、流通用記録媒体 $\alpha$ 上の当該コ

ンテンツファイルに係るヘッダ情報aに含まれる再生情報を主記憶部426上に読み出す一方、補助記憶部425から復号鍵c1を読み出し、当該復号鍵c1を用いて当該再生情報を復号化する。そして、当該再生情報を用いて流通用記録媒体 $\alpha$ 上のデータ本体bを復号化ビット長毎に主記憶部426に順次読み出すと共に、補助記憶部425から復号鍵c2を主記憶部426に読み出し、主記憶部426上の当該データを復号化ビット長毎に復号鍵c2を用いて順次復号化し、当該データをMPEG等のフィルタに通して圧縮状態から元の状態に順次復元し、これによりデータ本体bを再生する(s11)。

- [0166] このステップ11の処理と共に、流通用記録媒体 $\alpha$ からデータ本体bの開始位置情報を主記憶部426上に読み出す一方、補助記憶部425からピースデータdに含まれる位置情報を主記憶部426上に読み出し、当該開始位置情報から当該位置情報までのデータ長や時間のカウントを開始する(s12)。その後、前記カウントが終了したか否かを判定する(s13)。これにより、データ本体bの欠落部分の認識を行う。この判定の結果、カウントが終了したと判定してデータ本体bの欠落部分を認識すると、欠落データのビット長が復号化ビット長よりも小さい場合には、流通記録媒体 $\alpha$ からデータ本体bを、補助記憶部425からピースデータdに含まれる欠落データを主記憶部426上に読み出して(即ち、流通記録媒体 $\alpha$ 上のデータ本体bと補助記憶部425上の欠落データとを復号化ビット長のデータとして転送して)結合する(s14)。そして、当該主記憶部426上の復号化ビット長のデータを復号鍵c2を用いて復号化し(s15)、当該データをMPEG等のフィルタに通して圧縮状態から元の状態に復元し(s16)、これによりデータ本体bを再生する(s17)。

- [0167] 欠落データのビット長が復号化ビット長よりも大きい場合には、流通記録媒体 $\alpha$ からデータ本体bを、補助記憶部425からピースデータdに含まれる欠落データの一部を主記憶部426上に読み出して(即ち、流通記録媒体 $\alpha$ 上のデータ本体bと補助記憶部425上の欠落データの一部とを復号化ビット長のデータとして転送して)結合し、続いて、補助記憶部425からピースデータdに含まれる残りの欠落データ(復号化ビット長分のデータ)を主記憶部426上に読み出す(s14)。そして、主記憶部426上のデータを復号化ビット長毎に復号鍵c2を用いて復号化し(s15)、当該データをMPEG等

のフィルタに通して圧縮状態から元の状態に復元し(s16)、これによりデータ本体bを再生する(s17)。

[0168] 又は、補助記憶部425からピースデータdに含まれる欠落データの一部(復号化ビット長分のデータ)を主記憶部426上に読み出し、続いて、流通記録媒体 $\alpha$ からデータ本体bを、補助記憶部425からピースデータdに含まれる残りの欠落データを主記憶部426上に読み出して結合する(s14)。そして、主記憶部426上のデータを復号化ビット長毎に復号鍵c2を用いて復号化し(s15)、当該データをMPEG等のフィルタに通して圧縮状態から元の状態に復元し(s16)、これによりデータ本体bを再生する(s17)。このようにデータ本体bの欠落部分前後を再生した後、再び流通用記録媒体 $\alpha$ 上のデータ本体bを主記憶部426に読み出し、復号化ビット長毎に復号鍵c2を用いて順次復号化し、当該データをMPEG等のフィルタに通して圧縮状態から元の状態に順次復元し、これにより続きのデータ本体bを再生する(s18)。なお、欠落データのビット長が復号化ビットの2倍以上である場合、ステップ14の処理を連続して行う。この再生用ソフトウェアのプログラムはユーザにより終了の処理が行われることにより終了する。

[0169] また、再生用ソフトウェアには、上述した基本的な内容の他、デジタルコンテンツ再生装置420の電源がONにされると、デジタルコンテンツ再生装置420に常駐し、ピースデータdの管理を行う内容が含まれている。この内容においては、補助記憶部425上のピースデータdの管理を行う一方、ピースデータ送信日時と現在の日時との差をピースデータdが送信された時点からの経過期間として求め、これがレンタル情報に含まれるレンタル期間に達しているときはレンタル期間外であるとして補助記憶部425上のピースデータd及び復号鍵c1、c2を削除する一方、所定のフラグを倒すようになっている。

[0170] 復号鍵c2が盗まれ、ピースデータdを得ずにコンピュータ(デジタルコンテンツ再生装置420を含む)を用いて流通用記録媒体 $\alpha$ 上のコンテンツファイルのデータ本体bを不正に再生させようとする場合、コンピュータに再生ソフトウェアのステップ11と同じ処理を行わせ、これにより流通用記録媒体 $\alpha$ 上のコンテンツファイルのデータ本体bを再生させる。このとき、コンピュータの主記憶部上に復号化ビット長毎に読み出さ

れたデータが欠落部分の位置より前の位置のデータである場合、他のコンピュータの補助記憶部に予め記録させた盗んだ復号鍵c2を前記主記憶部に読み出させ、前記主記憶部上のデータを復号鍵c2を用いて復号化ビット長毎に復号化(即ち、所定の計算)させる。すると、盗んだ復号鍵c2を用いて復号化しているので、前記主記憶部上のデータを復号化ビット長毎に暗号化前のデータ列に順次変換させることができる。よって、その後、前記データをMPEG等のフィルタに通して圧縮状態から元の状態に復元させてデータ本体bを再生させることができる。

[0171] ところが、コンピュータの主記憶部上に読み出されたデータが欠落部分の位置より後ろの位置のデータである場合、他のコンピュータの補助記憶部から盗んだ復号鍵c2を主記憶部に読み出し、主記憶部上の当該データを復号鍵c2を用いて復号化ビット長毎に復号化(即ち、所定の計算)すると、前記主記憶部上のデータのデータ列が、図15に示すように、暗号化後のデータ列(即ち、欠落させる前のデータ列)と異なるデータ列であるので、不明な数列又は英数列に変換される。このような不明な数列又は英数列をMPEG等のフィルタを通すと、コンピュータの復元処理がストップする。このため、データ本体bの欠落部分以降のデータを再生することが不可能になる。

[0172] このようなデジタルコンテンツの不正使用防止システム400においては、不正使用防止システム100と同じ効果を得ることができる。

[0173] しかも、デジタルコンテンツの不正使用防止システム400では、コンテンツファイルのデータ本体bが圧縮され、暗号化された後、当該データ本体bの一部を欠落され、この欠落部分を連続するように詰めた状態で流通用記録媒体αに記録されている。このため、万一、復号鍵c2が盗まれ、これによりデータ本体bがコンピュータ等で不正に再生されたとしても、流通用記録媒体α上のコンテンツファイルのデータ本体bの欠落以降のデータが前記コンピュータの主記憶部上に復号化ビット長毎に読み出され、当該データが復号化ビット長毎に復号化されると、不明な数列又は英数列に変換される。この不明な数列又は英数列をMPEG等のフィルタに通すと、復元処理がストップするので、欠落部分以降のデータが再生できなくなる。このようにコンピュータ等の機器で大容量のデータを処理させるに当たり、前記機器の主記憶部上にデータを復号化ビット長毎に読み出させ、復号化ビット長毎に復号化して処理する当該機



器の特性をうまく生かしてデータ本体bの不正再生を防止することができるようになっている。しかも、データ本体bは欠落部分を連続するように詰めた状態で記録されている。即ち、このようなデータ本体bはデジタルデータであり英数字が連続するだけであるから、欠落部分を連続するように詰めると、当該欠落部分の位置を特定することができない。よって、当該欠落部分の位置を特定し、欠落部部より前の位置のデータを再生することもが困難である。更に、暗号化前にデータ本体bの一部を欠落させ、当該欠落部分にダミーデータ等を入れる又は欠落したままにすると、データ本体bをMPEGを用いて圧縮している場合、盗まれた復号鍵c2により欠落部分以外のデータ本体bが再生可能となってしまうが、データ本体bを暗号化後にその一部を欠落させ、この欠落部分の間を連続するように詰めると、欠落部分以降を再生することが不可能になるので、データ本体bの不正使用を防止する上で非常にメリットがある。

- [0174] デジタルコンテンツの不正使用防止システム400における流通用記録媒体 $\alpha$ については、データ本体bが圧縮され、暗号化され、当該データ本体bの一部が欠落され、当該欠落部分を連続するように詰められた状態で記録されているとしたが、圧縮を行うか否かは任意である。但し、圧縮しない場合には、欠落部分以降のデータ本体bは連続する不明な数列又は英数列の羅列として再生されることになる。圧縮方式としてはMPEGを例示したが、他の形式を用いることも当然可能である。また、コンテンツファイルはヘッダ情報a及びデータ本体bを有する構成であるとしたが、その他の情報を付加した状態で記録することは勿論可能である。その他の情報としては、ユーザのコンピュータに再生用ソフトウェアがインストールされているか否かを判断して、インストールされていないと判断した場合には、管理センタ410のHPに自動的にアクセスするプログラム等がある。このプログラムを記録させておくと、ユーザが自己のコンピュータ(デジタルコンテンツ再生装置420に相当するコンピュータであり、再生用ソフトウェアがダウンロードされていない状態)に予め入手した流通用記録媒体 $\alpha$ をセットすると、管理センタ410のWEBアドレスを読み出し、これに基づいて管理センタ410にアクセスする。その後、上述した手順で再生用ソフトウェアを入手することができる。

- [0175] 位置情報については、開始位置情報から欠落部分までのデータ長や時間であると

したが、欠落部分を示すアドレス値等であっても良い。この場合、次に読み出すべき流通用記録媒体 $\alpha$ 上のデータ本体bのアドレス値と位置情報とが一致するか否かを逐次判定し、この判定の結果、一致しないと判定したときには前記アドレス値の示す流通用記録媒体 $\alpha$ 上のデータ本体bを読み出し、一致すると判定したときには補助記憶部425上の欠落データを読み出すようにする。

[0176] ピースデータdについては、欠落データとその位置情報とからなるとしたが、前記位置情報を含めるか否かは任意である。この場合、例えば、予めデータ本体bの欠落部分の前に欠落部分であることを示す欠落位置情報を記録しておき、データ本体bを再生すると共に、開始位置情報から欠落位置情報までをカウントし、このカウントが終了すると、補助記憶部425上の欠落データを当該欠落部分のデータとして再生するようにすれば良い。或いは、予めデータ本体bの欠落部分の位置を決定しておく一方、再生用ソフトウェアに欠落データの位置情報が予め用意しておく。そして、データ本体bを再生すると共に、この位置情報に基づいてデータ本体bの欠落部分を認識し、補助記憶部425上の欠落データを当該欠落部分のデータとして再生するようにすることもできる。

[0177] ユーザ登録用割込プログラム、再生用ソフトウェアダウンロード用割込プログラム及びピースデータ配信用割込プログラムについては、上述したものは一例であり、必要に応じて設計変更可能である。

[0178] また、コンテンツファイルをデジタルコンテンツ再生装置420の補助記憶部425に記録した場合には、レンタル期間が過ぎると、ピースデータdと共に、コンテンツファイルを削除するようにしても良し、ピースデータdとは別に、コンテンツファイルを受信した時点からの経過期間を求め、当該経過期間が所定期間に達したときは、当該コンテンツファイルを削除するようにしても良い。

[0179] なお、第4の実施の形態についても、レンタルではなく有償又は無償でユーザに譲渡された流通用記録媒体 $\alpha$ 上のコンテンツファイルの不正使用を防止するシステムに設計変更することも可能であり、この場合であっても上記と同様のメリットを奏する。この場合に使用される再生用ソフトウェアについては、レンタル期間の内外に応じた一連の処理を削除するだけの内容で良い。また、デジタルコンテンツ再生装置に関

しては、再生用ソフトウェアを管理センタ410からダウンロードするのではなく、CD等の記録媒体を通じてインストールするようにしても良い。また、コンピュータではなく専用装置とすることも可能であるのは当然であり、ユーザにより認証及び課金を条件としたコンテンツファイルの再生の申し込みが入力されると、当該申し込みを通信回線 $\beta$ を介して管理センタ410に送信し、その後、管理センタ410からピースデータdが通信回線 $\beta$ を介して送信されると、再生操作時に流通用記録媒体 $\alpha$ 上のヘッダ情報及び当該ピースデータdを用いて流通用記録媒体 $\alpha$ 上のデータ本体bを再生するという機能を有する限り、どのような構成のものを用いてもかまわない。

### 実施例 5

[0180] 次に、本発明の第5の実施の形態を図面を参照しながら説明する。図17は本発明の第5の実施の形態に係るデジタルコンテンツの不正使用防止システムの構成図、図18は同システムに使用される再生用ソフトウェアのフローチャートである。

[0181] 図17に示すデジタルコンテンツの不正使用防止システム500は不正使用防止システム200と同じ構成である。異なる点は、コンテンツファイルの構成、デジタルコンテンツ再生装置520の補助記憶部525に記録される再生用ソフトウェアの内容(図18参照)である。以下、その相違点について詳しく説明し、重複する部分については説明を省略する。

[0182] コンテンツファイルは、実施例4と同様に、流通用記録媒体作成装置140によりヘッダ情報aが当該ヘッダ情報aに含まれる再生情報が暗号化された状態で記録媒体に記録される一方、データ本体bが、MPEG等の圧縮方式で圧縮され、暗号化され、当該データ本体bの一部が欠落され、当該欠落部分を連続するように詰められ、その後端に欠落させた部分と同ビット長のダミーデータが付加された状態で新たに設けたデータ本体用メモリ部(図示せず)に記録される。その後、流通用記録媒体作成装置140のデータ本体用メモリ部上のデータ本体bは通信回線 $\beta$ を介して配信管理センタ510に転送され、配信管理センタ510(電子機器)のデジタルコンテンツDB511(補助記憶装置)に記録される。なお、データ本体bを記録媒体に記録させて配信管理センタ510に郵送し、リードさせることにより、デジタルコンテンツDB511に記録させるようにしても良い。

- [0183] デジタルコンテンツ再生装置520はユーザが使用する汎用のコンピュータである。図中521はCPU等の制御部、522はモニタやスピーカ等の出力部、523はキーボードやマウス等の操作部、524は記録媒体等に対してデータのリード／ライトを行う再生複写部、525はハードディスク等の補助記憶部、526は通信回線 $\beta$ に接続されており且つ通信を行うための通信部、527はDRAM等の主記憶部である。
- [0184] 補助記憶部525にはコンピュータとしてのオペレーションシステム等の基本プログラム以外に図18に示す再生用ソフトウェアが記録されている。再生用ソフトウェアの内容については後述するが、当該再生用ソフトウェアが制御部521に主記憶部527上で処理されることにより、補助記憶部525又は記録媒体に記録されたデータ本体bを主記憶部426に復号化ビット長毎に順次転送させ、主記憶部426上の当該データを復号化ビット長毎に順次復号化(即ち、復号化ビット長毎に復号化)させ、当該データを圧縮状態から元の状態に戻して再生(リード)するデジタルコンテンツ再生装置520としての機能を発揮するようになっている。
- [0185] 以上のように構成されたデジタルコンテンツの不正使用防止システム500のデジタルコンテンツ再生装置520を用いたデジタルコンテンツの不正使用防止方法を説明すると共に、配信管理センタ510の動作、デジタルコンテンツ再生装置520の動作及び各プログラムの内容について説明する。暗号鍵c1、c2は配信管理センタ510のピースデータDB516に記録されているものとする。以下、説明の便宜上、データ本体bは一箇所のみ欠落しているものとして説明する。
- [0186] まず、デジタルコンテンツ再生装置520には、実施例2と同様の手順で再生用ソフトウェアがダウンロードされ、補助記憶部525に記録されている。そして、実施例2と同様の手順でコンテンツファイルを配信管理センタ510のデジタルコンテンツDB511からダウンロードし、デジタルコンテンツ再生装置520の補助記憶部525又は記録媒体に記録させている。
- [0187] その後、このデジタルコンテンツ再生装置520は、ユーザにより再生用ソフトウェアが実行される(コンテンツファイルを記録媒体に記録した場合には再生用ソフトウェアが実行される一方で当該記録媒体が再生複写部524にセットされる。)と、当該再生用ソフトウェアに含まれる再生プレーヤ、プレイリスト等のデータを出力部522に表示

出力する。すると、再生プレーヤの画面上にプレイリストが表示される(s1)。このプレイリストにはダウンロードしたコンテンツファイルのファイル名と共に、当該コンテンツファイルがレンタル中であるか否かが表示される。即ち、再生の申込がされたことを示す所定のフラグが立っているコンテンツファイルがレンタル中であるとして表示される。そして、このプレイリストに基づき操作部523を通じてレンタル中のコンテンツファイルが再生操作されたか否かを判定する(s2)。

[0188] 再生操作がなされていないと判定すると、操作部523を通じてプレイリストに表示されたレンタル中でないコンテンツファイルの再生の申し込み操作されたか否かを判定する(s3)。その結果、再生の申し込み操作がなされていないと判定すると、操作部523を通じて記録媒体の読み込みの操作(DISC LOADの操作)がなされたか否かを判定する(s4)。DISC LOADの操作がなされると、プレイリストに記録されていない記録媒体上の(即ち、他のコンピュータ等で記録媒体上にダウンロードした)コンテンツファイルを示すコンテンツリストを出力部522に表示出力する(s5)。即ち、記録媒体上のコンテンツファイルのうち所定のフラグが立っていないコンテンツファイルのヘッダ情報aに含まれるコンテンツ情報を主記憶部527上に読み出し、コンテンツリストに表示する。

[0189] その後、ユーザによりプレイリスト上のレンタル中でないコンテンツファイル又はコンテンツリスト上のコンテンツファイルの再生の申し込みがなされると(s3又はs6)、補助記憶部525又は記録媒体上の当該コンテンツファイルのヘッダ情報aに含まれるコンテンツ情報を主記憶部427上に読み出す。そして、当該コンテンツ情報に含まれるのWEBアドレスに基づき当該コンテンツ情報に含まれるコンテンツIDを通信回線 $\beta$ を介して配信管理センタ510に送信する。このようにして再生申込処理を行う旨を送信する。

[0190] すると、配信管理センタ510はピースデータ配信用割込プログラムを処理する(図9参照)。そして、メモリ部516から再生申込処理に必要なデータを読み出し、通信回線 $\beta$ を介してデジタルコンテンツ再生装置520に送信する(

s31)。デジタルコンテンツ再生装置520は、このデータに基づいて再生申込用画面のデータを主記憶部426上に読み出し、出力部522に表示出力する(s7)。

[0191] その後、ユーザが再生申込用画面が示すところに従ってレンタル期間を操作部523を通じて順次入力又は選択(これによりレンタル金額が自動的に決まる)し、最後にユーザIDやパスワードをコンテンツファイルの再生申し込みとして操作部523を通じて入力すると(s8)、デジタルコンテンツ再生装置520は、出力部522の表示出力を認証画面に切り換える一方、入力された申し込みデータを通信回線βを介して配信管理センタ510に送信する。この際、補助記憶部525又は記録媒体上のコンテンツ情報のコンテンツIDと当該補助記憶部525上のプレーヤIDとを読み出し、申し込みデータと一緒に配信管理センタ510に送信する(s9)。

[0192] すると、配信管理センタ510は、当該記申し込みデータ等を受信すると、当該申し込みに係るユーザの認証を確認する(s32)。即ち、受信したユーザのユーザIDやプレーヤID等を参照してユーザ情報DB514から当該ユーザのユーザ情報を読み出し、当該ユーザが真正のユーザであるか否かを確認する。このとき、配信管理センタ510は、ユーザ情報DB514にレンタル料金の不払い等が所定以上ある不適当者リストが予め用意されており、当該認証と共に不適当者リストに該当する者でないか否かを確認する(

なお、不適当者リストの確認は任意である)。

[0193] 配信管理センタ510は、申し込みに係るユーザが不正なユーザである又は真正のユーザであるものの不適当者リストに該当する者であると確認した場合、ユーザの申し込みを拒否する旨を通信回線βを介してデジタルコンテンツ再生装置520に送信する(s33)。その後、ピースデータ配信用割込プログラムを処理を終了する。

[0194] 一方、申し込みに係るユーザが真正のユーザであり且つ不適当者リストに該当しない者であることを確認した場合、ユーザのプレーヤID等を参照して当該ユーザのユーザ情報DB514上のユーザ情報に課金を記録する一方、コンテンツIDを参照してピースデータDB216を検索し当該コンテンツIDに対応するピースデータd及び復号鍵c1、c2を読み出し、これを再生の申し込みデータに含まれるレンタル情報と共にユーザの申し込みを承諾する旨の回答として通信回線βを介してデジタルコンテン

ツ再生装置520に送信する(s34)。その後、ピースデータ配信用割込プログラムを処理を終了する。

- [0195] なお、課金については、所定期間毎にユーザ情報DB514に基き、銀行・カード会社530に請求するか若しくは、ユーザに直接請求し、ユーザに振込やコンビニエンスストア等で支払いをさせるようにする。また、配信管理センタ510が銀行・カード会社230と通信回線 $\beta$ を介して接続されている場合には、即時決済とすることももちろん可能である。
- [0196] デジタルコンテンツ再生装置520は、その後、通信回線 $\beta$ を介してユーザの申し込みを拒否する旨を受信すると(s10)、拒否する旨のデータに含まれるエラーメッセージのデータを出力部522に表示出力する(s11)。
- [0197] 一方、通信回線 $\beta$ を介してピースデータd、復号鍵c1、c2及びレンタル情報を受信すると(s10)、所定のフラグを立てる一方、ピースデータd、復号鍵c1、c2及びレンタル情報を補助記憶部525に記録する(s12)。と同時に、コンピュータの時計機能を用いてピースデータ送信日時を補助記憶部525に記録する。そして、プレイリストを更新して出力部522に表示出力し、当該プレイリスト中にピースデータdを得たコンテンツファイルのファイル名を表示させる(s1)。
- [0198] その後、デジタルコンテンツ再生装置520は、操作部523を通じてプレイリストに基づきレンタル中のコンテンツファイルの再生操作がなされると(s2)、補助記憶部525又は記録媒体上のコンテンツファイルのヘッダ情報aに含まれる再生情報を主記憶部527に読み出す一方、補助記憶部525上の復号鍵c1を主記憶部527に読み出す。そして、当該再生情報を用いて補助記憶部525又は記録媒体上のデータ本体bを復号化ビット長毎に主記憶部527上に順次読み出す一方、補助記憶部525から復号鍵c2を主記憶部527に読み出す。そして、主記憶部527の当該データを復号鍵c2を用いて復号化ビット長毎に復号化し、当該データをMPEG等のフィルタに通して圧縮状態から元の状態に復元し、これによりデータ本体bを再生する(s13)。
- [0199] と共に、補助記憶部525又は記録媒体上のデータ本体bの開始位置情報を主記憶部527に読み出す一方、補助記憶部525上のピースデータdに含まれる位置情報を主記憶部527に読み出し、当該開始位置情報から当該位置情報までのデータ長や

時間のカウントを開始する(s14)。その後、前記カウントが終了したか否かを判定する(s15)。これにより、データ本体bの欠落部分の認識を行う。この判定の結果、カウントが終了したと判定してデータ本体bの欠落部分を認識すると、欠落データのビット長が復号化ビット長よりも小さい場合には、補助記憶部525又は記録媒体からデータ本体bを、補助記憶部525からピースデータdに含まれる欠落データを主記憶部527に読み出して(即ち、記録媒体又は補助記憶部525上のデータ本体bと補助記憶部525上の欠落データとを復号化ビット長のデータとして転送して)結合する(s16)。そして、主記憶部527上の復号化ビット長のデータを復号鍵c2を用いて復号化し(s17)、当該データをMPEG等のフィルタに通して圧縮状態から元の状態に復元し(s18)、これによりデータ本体bを再生する(s19)。

[0200] 欠落データのビット長が復号化ビット長よりも大きい場合には、補助記憶部525又は記録媒体からデータ本体bを、補助記憶部525からピースデータdに含まれる欠落データの一部を主記憶部527上に読み出して(即ち、流通記録媒体 $\alpha$ 上のデータ本体bと補助記憶部525上の欠落データの一部とを復号化ビット長のデータとして転送して)結合し、続いて、補助記憶部525からピースデータdに含まれる残りの欠落データ(復号化ビット長分のデータ)を主記憶部527上に読み出す(s16)。そして、主記憶部527上のデータを復号化ビット長毎に復号鍵c2を用いて復号化し(s17)、当該データをMPEG等のフィルタに通して圧縮状態から元の状態に復元し(s18)、これによりデータ本体bを再生する(s19)。

[0201] 又は、補助記憶部525からピースデータdに含まれる欠落データの一部(復号化ビット長分のデータ)を主記憶部527上に読み出し、続いて、補助記憶部525又は記録媒体からデータ本体bを、補助記憶部525からピースデータdに含まれる残りの欠落データ主記憶部527上に読み出して結合する(s16)。そして、主記憶部527上のデータを復号化ビット長毎に復号鍵c2を用いて復号化し(s17)、当該データをMPEG等のフィルタに通して圧縮状態から元の状態に復元し(s18)、これによりデータ本体bを再生する(s19)。このようにデータ本体bの欠落部分前後を再生した後、再び補助記憶部525又は記録媒体上のデータ本体bを主記憶部527に読み出し、復号化ビット長毎に復号鍵c2を用いて順次復号化し、当該データをMPEG等のフィルタに通し



て圧縮状態から元の状態に順次復元し、これにより続きのデータ本体bを再生する(s20)。なお、欠落データのビット長が復号化ビットの2倍以上である場合、ステップ16の処理を連続して行う。この再生用ソフトウェアのプログラムはユーザにより終了の処理が行われることにより終了する。

[0202] また、再生用ソフトウェアには、上述した基本的な内容の他、デジタルコンテンツ再生装置520の電源がONにされると、当該デジタルコンテンツ再生装置520に常駐し、ピースデータdの管理を行う内容が付加されている。この内容においては、補助記憶部525上のピースデータdの管理を行う一方、ピースデータ送信日時と現在の日時との差をピースデータdが送信された時点からの経過期間として求め、これがレンタル情報に含まれるレンタル期間に達しているときはレンタル期間外であるとして補助記憶部525上のピースデータd及び復号鍵c1、c2を削除する一方、所定のフラグを倒すようになっている。

[0203] 復号鍵c2が盗まれ、ピースデータdを得ずにコンピュータ(デジタルコンテンツ再生装置520を含む)を用いて当該コンピュータの補助記憶部又は記録媒体に記録されたコンテンツファイルのデータ本体bを不正に再生させようとする場合、コンピュータに再生用ソフトウェアのステップ13と同じ処理を行わせ、これにより補助記憶部又は記録媒体上のコンテンツファイルのデータ本体bを再生させる。このとき、コンピュータの主記憶部上に復号化ビット長毎に読み出されたデータが欠落部分の位置より前の位置に記録されたデータである場合、他のコンピュータの補助記憶部に予め記録させた盗んだ復号鍵c2を前記主記憶部に読み出させ、前記主記憶部上のデータを復号鍵c2を用いて復号化ビット長毎に復号化(即ち、所定の計算)させる。すると、盗んだ復号鍵c2を用いて復号化しているので、前記データを暗号化前のデータ列に変換させることができる。よって、その後、前記データをMPEG等のフィルタに通して圧縮状態から元の状態に復元させてデータ本体bを再生させることができる。

[0204] ところが、コンピュータの主記憶部上に復号化ビット長毎に読み出されたデータが欠落部分の位置より後ろの位置に記録されたデータである場合、他のコンピュータの補助記憶部から盗んだ復号鍵c2を主記憶部に読み出し、当該主記憶部上のデータを復号鍵c2を用いて復号化ビット長毎に復号化(即ち、所定の計算)すると、前記主

記憶部上のデータのデータ列は、暗号化後のデータ列(即ち、欠落させる前のデータ列)と異なるデータ列である(図15を借りて参照)ので、不明な数列又は英数列に変換される。このような不明な数列又は英数列をMPEG等のフィルタを通すと、他のコンピュータの復元処理がストップする。このため、データ本体bの欠落部分以降のデータを再生することが不可能になる。

[0205] このようなこのようなデジタルコンテンツの不正使用防止システム500においては、不正使用防止システム200と同じ効果を得ることができる。

[0206] しかも、デジタルコンテンツの不正使用防止システム500では、コンテンツファイルのデータ本体bが圧縮され、暗号化された後、当該データ本体bの一部を欠落され、この欠落部分を連続するように詰めた状態で補助記憶部又は記録媒体に記録されている。このため、万一、復号鍵c2が盗まれ、これによりデータ本体bがコンピュータ等で不正に再生されたとしても、補助記憶部又は記録媒体上のコンテンツファイルのデータ本体bの欠落部分以降のデータが前記コンピュータの主記憶部上に復号化ビット長毎に読み出され、復号化ビット長毎に復号化されると、不明な数列又は英数列に変換される。この不明な数列又は英数列をMPEG等のフィルタに通すと、復元処理がストップするので、欠落部分以降のデータが再生できなくなる。このようにコンピュータ等の機器で大容量のデータを処理させるに当たり、前記機器の主記憶部上にデータを復号化ビット長毎に読み出させて処理する当該機器の特性をうまく生かしてデータ本体bの不正再生を防止することができるようになっている。しかも、データ本体bは欠落部分を連続するように詰めた状態で記録されている。即ち、このようなデータ本体bはデジタルデータであり英数字が連続するだけであるから、欠落部分を連続するように詰めると、当該欠落部分の位置を特定することができない。よって、当該欠落部分の位置を特定し、欠落部分より前の位置のデータを再生することも困難である。更に、暗号化前にデータ本体bの一部を欠落させ、当該欠落部分にダミーデータ等を入れる又は欠落したままにすると、データ本体bをMPEGを用いて圧縮している場合、盗まれた復号鍵c2により欠落部分以外のデータ本体bが再生可能となってしまうが、データ本体bを暗号化後にその一部を欠落させ、この欠落部分の間を連続するように詰めた状態で記録されていると、欠落部分以降を再生することが不可能にな

るので、データ本体bの不正使用を防止する上で非常にメリットがある。

[0207] また、デジタルコンテンツDB511には、データ本体bが圧縮され、暗号化され、当該データ本体bの一部が欠落され、当該欠落部分を連続するように詰められた状態で記録されているとしたが、圧縮を行うか否かは任意である。但し、圧縮しない場合には、欠落部分以降のデータ本体bは連続する不明な数列又は英数列の羅列として再生されることになる。圧縮方式としてはMPEGを例示したが、他の形式を用いることも当然可能である。また、コンテンツファイルはヘッダ情報a及びデータ本体bとを有する構成であるとしたが、その他の情報を付加した状態で記録することは勿論可能である。その他の情報としては、ユーザのコンピュータに再生用ソフトウェアがインストールされているか否かを判断して、インストールされていないと判断した場合には、配信管理センタ510のHPに自動的にアクセスするプログラム等がある。このプログラムを記録させておくと、ユーザが自己のコンピュータ(デジタルコンテンツ再生装置520に相当するコンピュータであり、再生用ソフトウェアがダウンロードされていない状態)に予め入手したコンテンツファイルを実行しようとする、配信管理センタ510のWEBアドレスを読み出し、これに基づいて配信管理センタ510に自動的にアクセスする。その後、上述した手順で再生用ソフトウェアを入手するようにすることができる。

[0208] 位置情報については、開始位置情報から欠落部分までのデータ長や時間であるとしたが、欠落部分を示すアドレス値等であっても良い。この場合、次に読み出すべき流通用記録媒体 $\alpha$ 上のデータ本体bのアドレス値と位置情報とが一致するか否かを逐次判定し、この判定の結果、一致しないと判定したときには前記アドレス値の示す補助記憶部525又は記録媒体上のデータ本体bを読み出し、一致すると判定したときには補助記憶部525上の欠落データを読み出すようにする。

[0209] ピースデータdについては、欠落データとその位置情報とからなるとしたが、前記位置情報を含めるか否かは任意である。この場合、例えば、予めデータ本体bの欠落部分の前に欠落部分であることを示す欠落位置情報を記録しておき、データ本体bを再生すると共に、開始位置情報から欠落位置情報までをカウントし、このカウントが終了すると、補助記憶部525上の欠落データを当該欠落部分のデータとして再生するようにすれば良い。或いは、予めデータ本体bの欠落部分の位置を決定しておくと共に

に、再生用ソフトウェアに欠落データの位置情報が予め用意しておく。そして、データ本体bを再生すると共に、この位置情報に基づいてデータ本体bの欠落部分を認識し、補助記憶部525上の欠落データを当該欠落部分のデータとして再生するようにすることもできる。

- [0210] ユーザ登録用割込プログラム、再生用ソフトウェアダウンロード用割込プログラム及びピースデータ配信用割込プログラムについては、上述したものは一例であり、必要に応じて設計変更可能である。
- [0211] このデータの不正使用防止方法、プログラムについては、実施例3のデジタルコンテンツ再生装置320にも適応可能であることは言う迄もない。
- [0212] また、コンテンツファイルをデジタルコンテンツ再生装置520の補助記憶部525に記録した場合には、レンタル期間が過ぎると、ピースデータdと共に、コンテンツファイルを削除するようにしても良し、ピースデータdとは別に、コンテンツファイルを受信した時点からの経過期間を求め、当該経過期間が所定期間に達したときは、当該コンテンツファイルを削除するようにしても良い。
- [0213] なお、第5の実施の形態についても、レンタルではなく有償又は無償で配信されたコンテンツファイルの不正使用を防止するシステムに設計変更することも可能であり、この場合であっても上記と同様のメリットを奏する。この場合に使用される再生用ソフトウェアについては、配信されたコンテンツファイルがレンタル期間外であるときの処理を削除するだけの内容で良い。また、デジタルコンテンツ再生装置520に関しては、再生用ソフトウェアを配信管理センタ510からダウンロードするのではなく、CD等の記録媒体を通じてインストールするようにしても良い。また、コンピュータではなく専用装置の形態にすることもできるのは当然である。
- [0214] 以上の実施例では、デジタルコンテンツのデータ本体bを加工する方法として説明したが、暗号化されており且つ復号化ビット長毎に複合化され、これによりリードされるデータの加工方法において、データを暗号化し、このデータの復号化ビット長と異なるビット長の一部を欠落させ、その欠落部分の間を詰めて当該データを連続させる限りどのようなデータでも加工することが可能である。データを加工する機器については、流通用記録媒体作成装置140と同様の機能を実現できるものであればどのよう

なものをを用いても良い。例えば、コンピュータであるデータリード装置に上記方法を用いてデータを加工させることができる。

- [0215] また、このデータの加工方法は送受信されるデータの不正使用を防止する方法として利用可能である。この場合、デジタルコンテンツ再生装置はデータをリードできるデータリード装置であれば良く、管理センタ及び配信管理センタは、データリード装置と通信回線を介して接続されており且つ欠落データを記録する補助記憶装置を有する電子機器であれば良い。なお、前記電子機器はデータリード装置を含む概念である。具体的には、データリード装置の補助記憶部に記録されたデータを電子機器に送信するに当たり、データを暗号化させ、当該データの少なくとも一部を欠落させ、当該欠落部分の間を連続するように詰めさせ、当該データを自身の補助記憶部に記憶させる一方、欠落データを当該欠落データがデータのどの部分であるかを示す位置情報と共に補助記憶部に記録させる。その後、データリード装置に補助記憶部上の前記データを電子機器に送信させる一方、欠落データ、位置情報及び復号鍵を前記データとは別に前記他のデータリード装置に送信させる。このようにすることにより、データを安全に他のデータリード装置に送信することができ、万一、データ及び暗号鍵が盗まれたとしても、欠落データ及び位置情報を得ない限りリードすることはできず、データの不正使用を防止することができる。なお、欠落データ及び位置情報と復号鍵とは別々に送信することが望ましいことはいうまでもない言う迄もない。

### 請求の範囲

- [1] 暗号化されており且つ復号化ビット長毎に複合化され、これによりリードされるデータの加工方法において、データを暗号化し、このデータの復号化ビット長と異なるビット長の一部を欠落させ、その欠落部分の間を詰めて当該データを連続させたことを特徴とするデータの加工方法。
- [2] 請求項1記載のデータの加工方法において、前記データを暗号化する前に、圧縮するようにしたことを特徴とするデータの加工方法。
- [3] 請求項1又は2記載の加工方法において、前記データの欠落部分の間を詰めて連続させた後、当該データの後端に欠落データと同じビット長のダミーデータを付加するようにしたことを特徴とするデータの加工方法。
- [4] 請求項1のデータの加工方法において、欠落データのビット長を、復号化ビット長の約数と異なるビット長としたことを特徴とするデータの加工方法。
- [5] データを複数箇所欠落させた請求項3のデータの加工方法において、欠落データのビット長×欠落箇所数を、復号化ビット長の約数と異なるビット長としたことを特徴とするデータの加工方法。
- [6] 請求項1のデータの加工方法により加工され、且つ記録媒体又はデータリード装置の補助記憶部に予め記録されたデータをデータリード装置を用いてリードするデータのリード方法であって、欠落データと当該欠落データがデータのどの部分であることを示す位置情報とが予め記録された補助記憶装置を有する電子機器と、この電子機器と通信回線を介して接続された前記データリード装置とを備えるシステムであって、  
データリード装置は操作入力に応じてリードするデータに係る欠落データ及びその位置情報を電子機器に通信回線を介して要求し、電子機器は当該要求に応じて欠落データ及びその位置情報を同時又は相前後して送信し、

データリード装置は欠落データ及びその位置情報を受信して補助記憶部に記録し

その後、記録媒体又は補助記憶部上のデータを主記憶部に順次転送し、主記憶部上のデータを復号化ビット長毎に順次復号化してリードするに当たり、

補助記憶部上の位置情報を主記憶部に転送し、当該位置情報を参照して前記データの欠落部分を認識し、補助記憶部上の欠落データを主記憶部に転送する一方、記録媒体又は補助記憶部上のデータを当該主記憶部に転送し、当該主記憶部上でデータの当該欠落部分に当該欠落データを結合し、当該データを復号化ビット長毎に復号化するようにしたことを特徴とするデータのリード方法。

- [7] 請求項2のデータの加工方法により加工され、且つ記録媒体又はデータリード装置の補助記憶部に予め記録されたデータをデータリード装置を用いてリードするデータのリード方法であって、欠落データと当該欠落データがデータのどの部分であるかを示す位置情報とが予め記録された補助記憶装置を有する電子機器と、この電子機器と通信回線を介して接続された前記データリード装置とを備えるシステムであって、

データリード装置は操作入力に応じてリードするデータに係る欠落データ及びその位置情報を電子機器に通信回線を介して要求し、電子機器は当該要求に応じて欠落データ及びその位置情報を同時又は相前後して送信し、

データリード装置は欠落データ及びその位置情報を受信して補助記憶部に記録し

その後、記録媒体又は補助記憶部上のデータを主記憶部に順次転送し、主記憶部上のデータを復号化ビット長毎に順次復号化し、当該データを圧縮状態から元の状態に復元してリードするに当たり、

補助記憶部上の位置情報を主記憶部に転送し、当該位置情報を参照して前記データの欠落部分を認識し、補助記憶部上の欠落データを主記憶部に転送する一方、記録媒体又は補助記憶部上のデータを当該主記憶部に転送し、当該主記憶部上でデータの当該欠落部分に当該欠落データを結合し、当該データを復号化ビット長毎に復号化し、当該データを圧縮状態から元の状態に復元するようにしたことを特徴

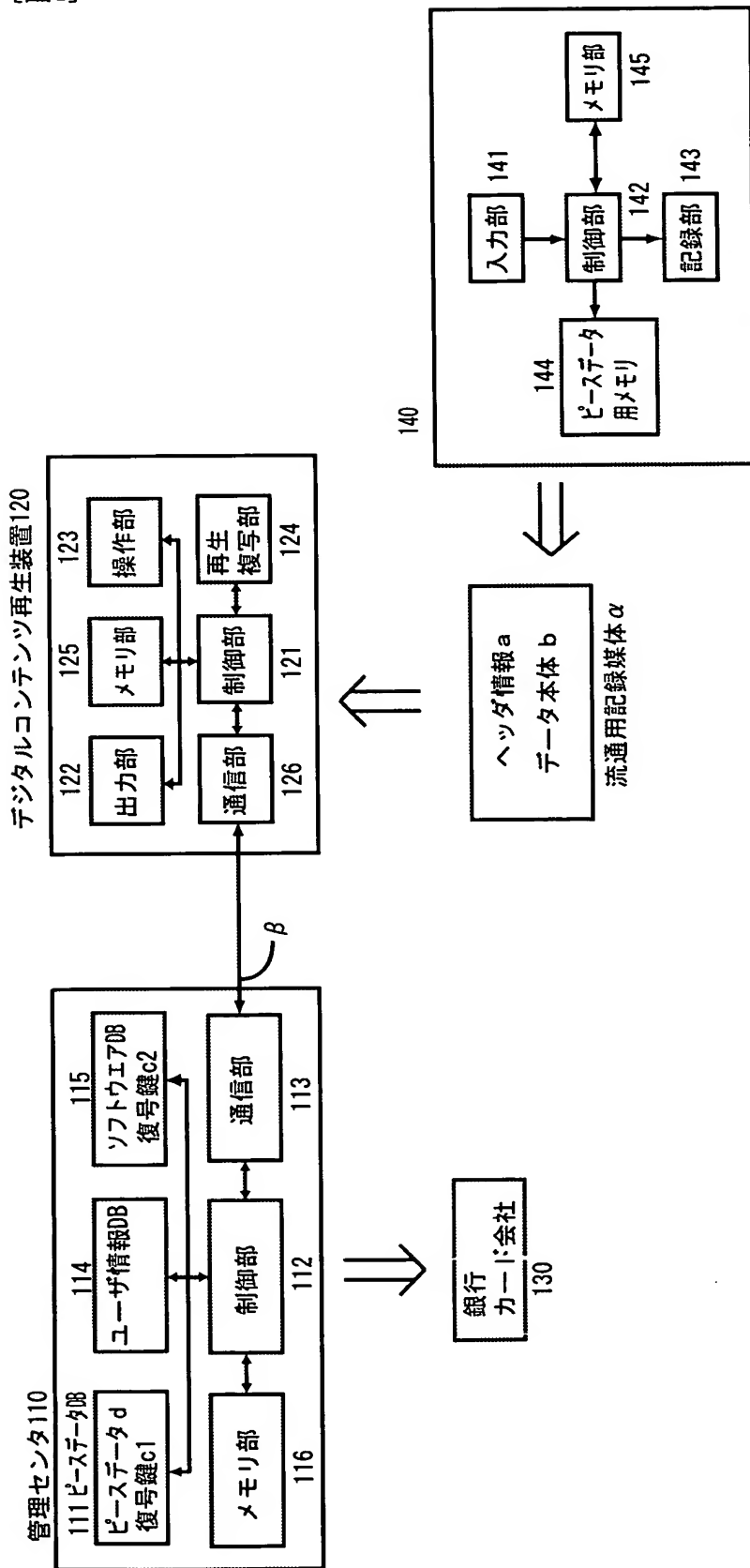
とするデータのリード方法。

- [8] 請求項6又は7記載のデータのリード方法において、前記電子機器は、欠落データ及び位置情報の送信によりデータの使用を管理する管理手段であることを特徴とするデータのリード方法。
- [9] 請求項6又は7記載のデータのリード方法において、記録媒体又はデータリード装置の補助記憶部に記録されたデータは、電子機器の前記補助記憶装置又は別の補助記憶装置に予め記録されており、データリード装置の電子機器に対する通信回線を介した要求に応じて電子機器から送信され、記録媒体又は前記データリード装置の補助記憶部に記録されることを特徴とするデータのリード方法。
- [10] 請求項6又は7記載のデータのリード方法において、データリード装置に欠落データを受信した時点からの経過期間を求めさせ、当該経過期間が所定期間に達したときは、少なくとも補助記憶部上の欠落データを削除させるようにしたことを特徴とするデータのリード方法。
- [11] 請求項10記載のデータのリードにおいて、データリード装置に、欠落データとは別にデータを受信した時点からの経過期間を求めさせ、当該経過期間が所定期間に達したときは、補助記憶部上のデータを削除させるようにしたことを特徴とするデータのリード方法。
- [12] 請求項1、2、3、4、5又は6記載のデータの加工方法を実現するプログラムが記録されたことを特徴とする記録媒体。
- [13] 請求項7、8、9、10又は11記載のデータのリード方法を実現するプログラムが記録されたことを特徴とする記録媒体。

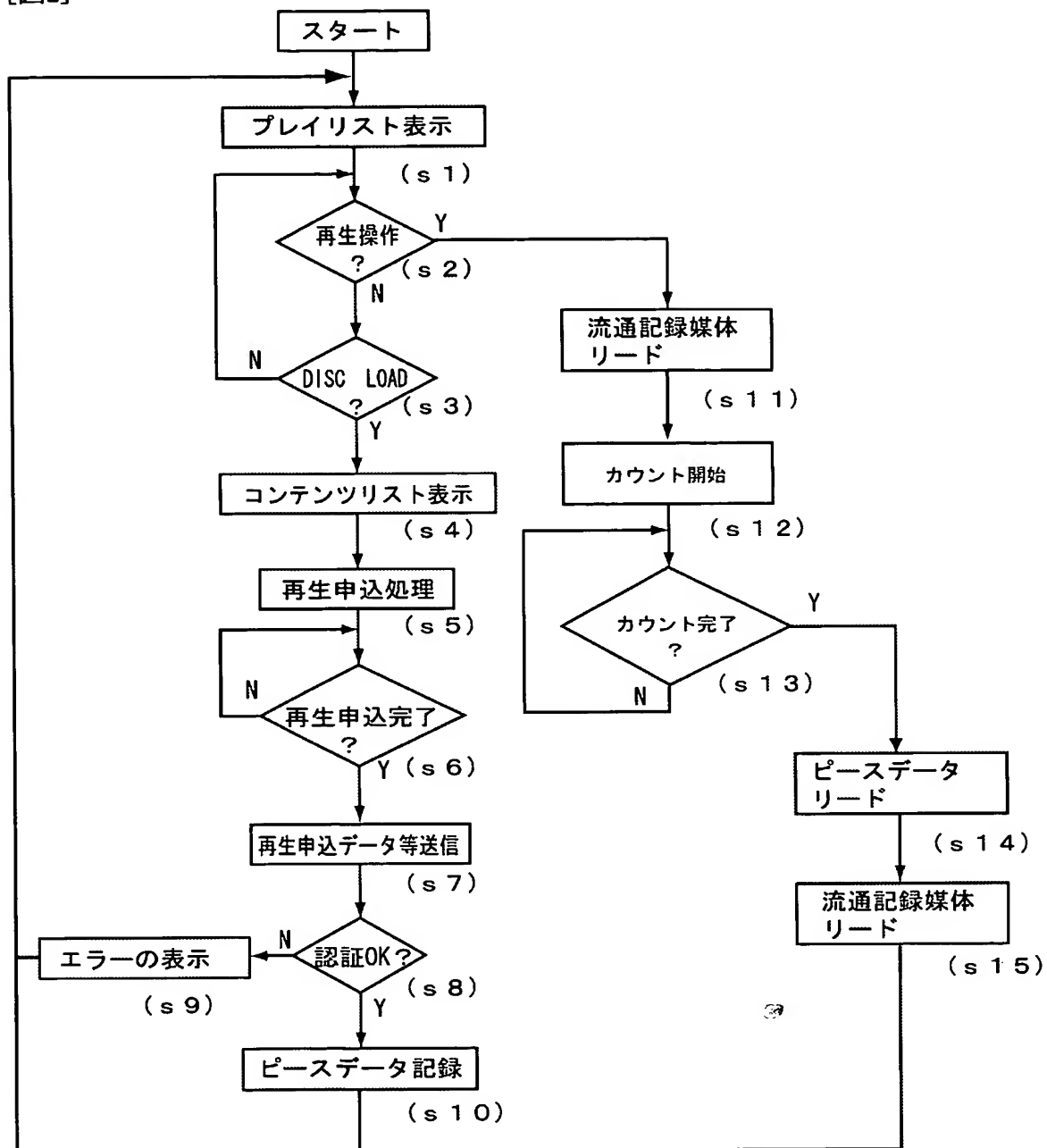


[図1]

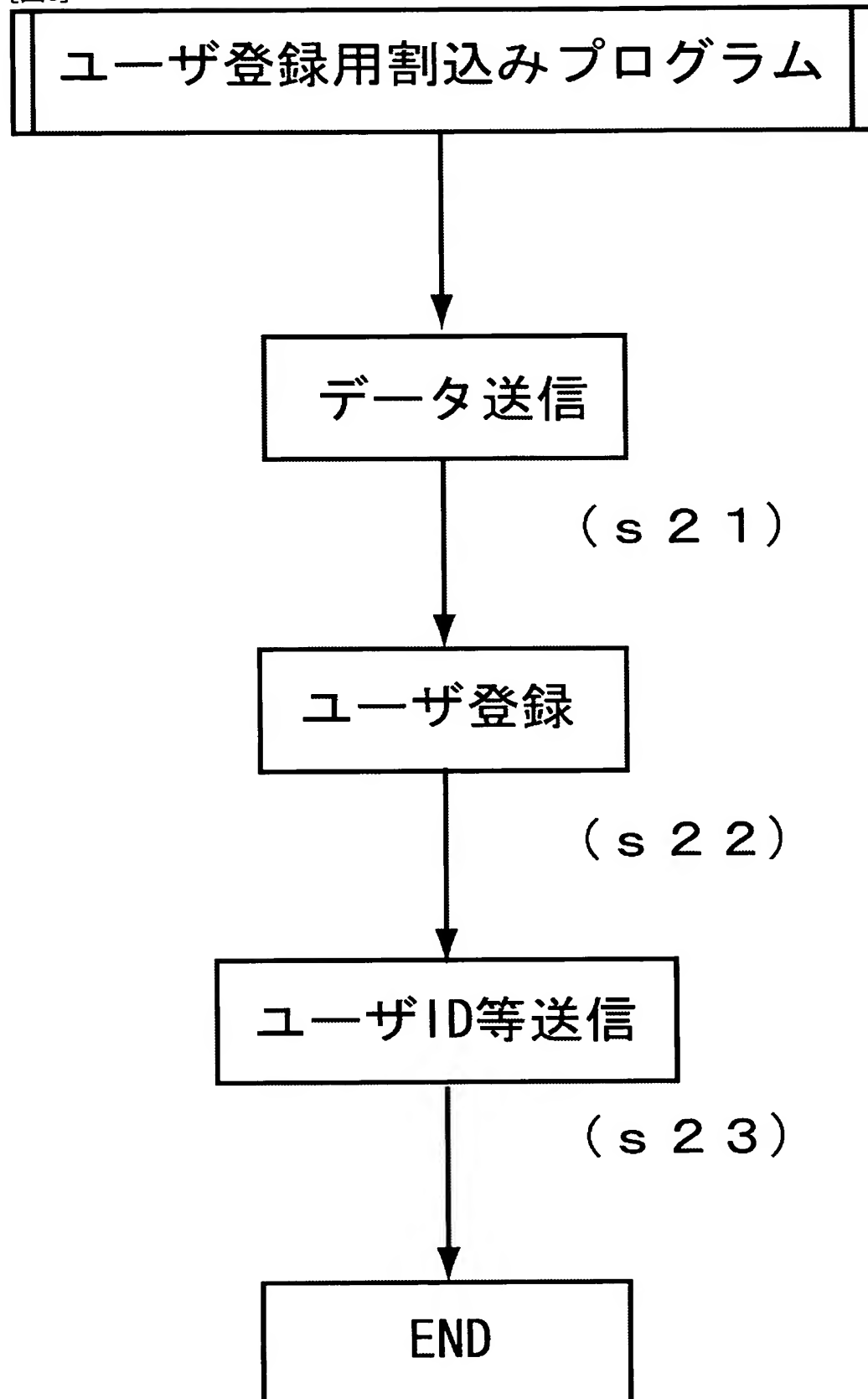
100



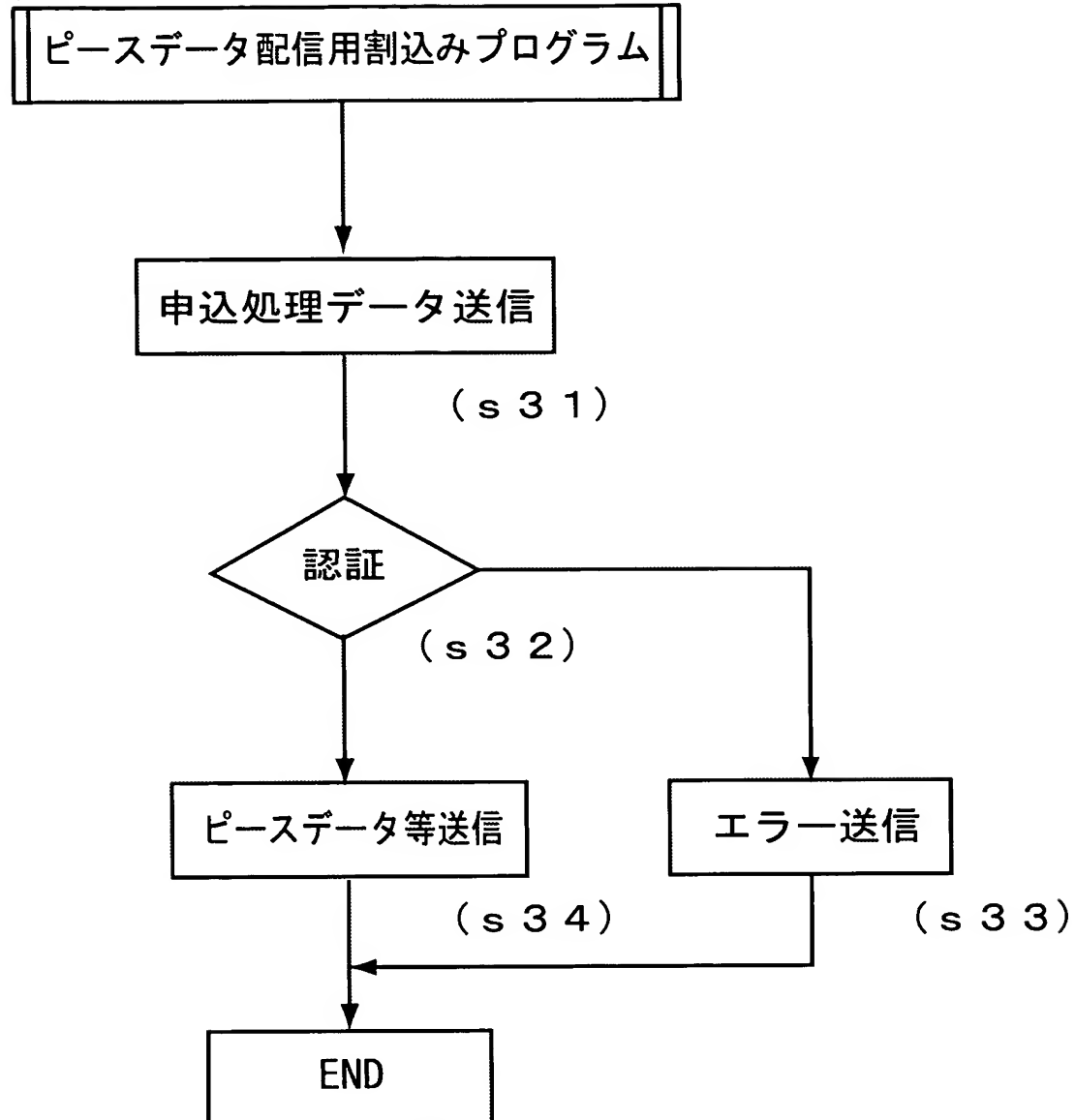
[図2]



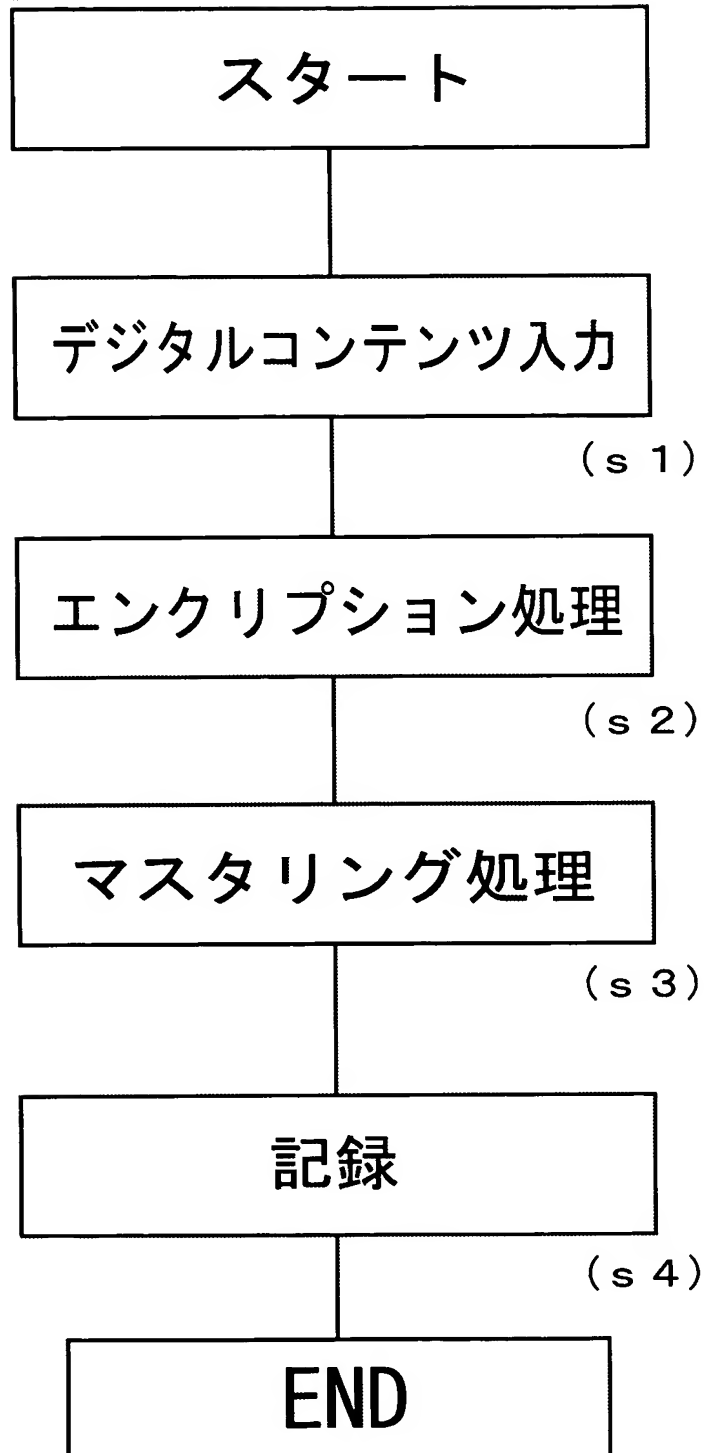
[図3]

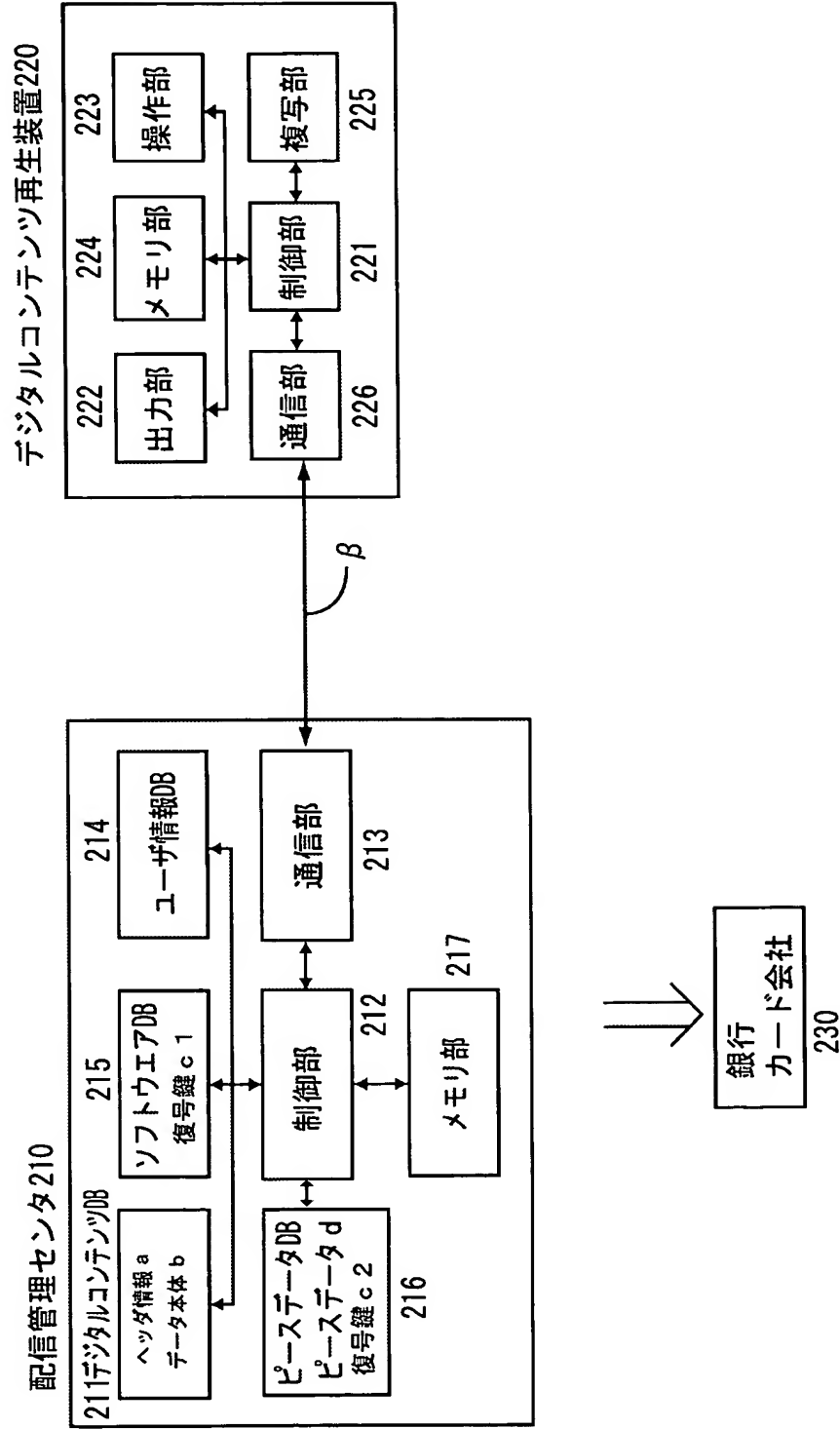


[図4]

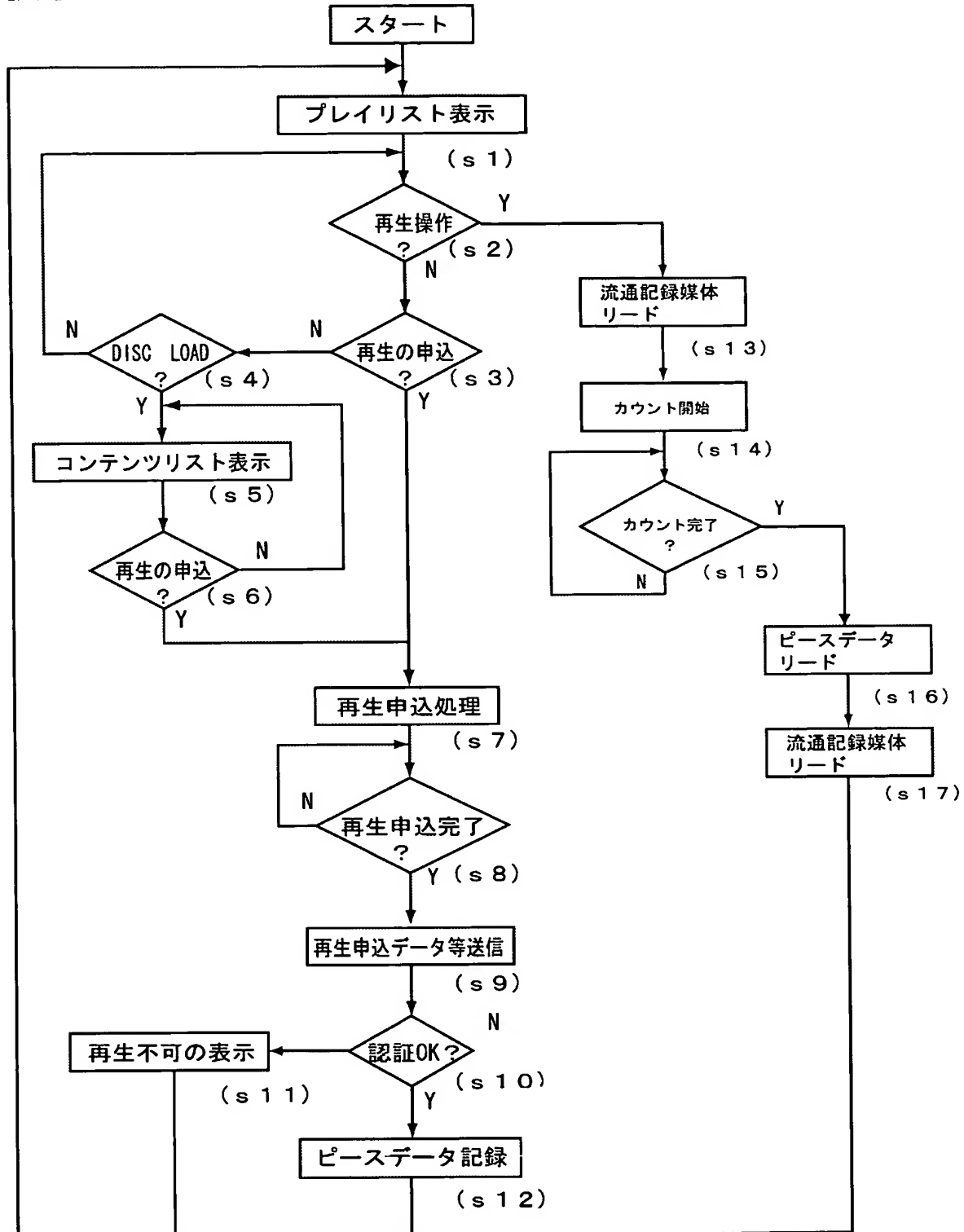


[図5]

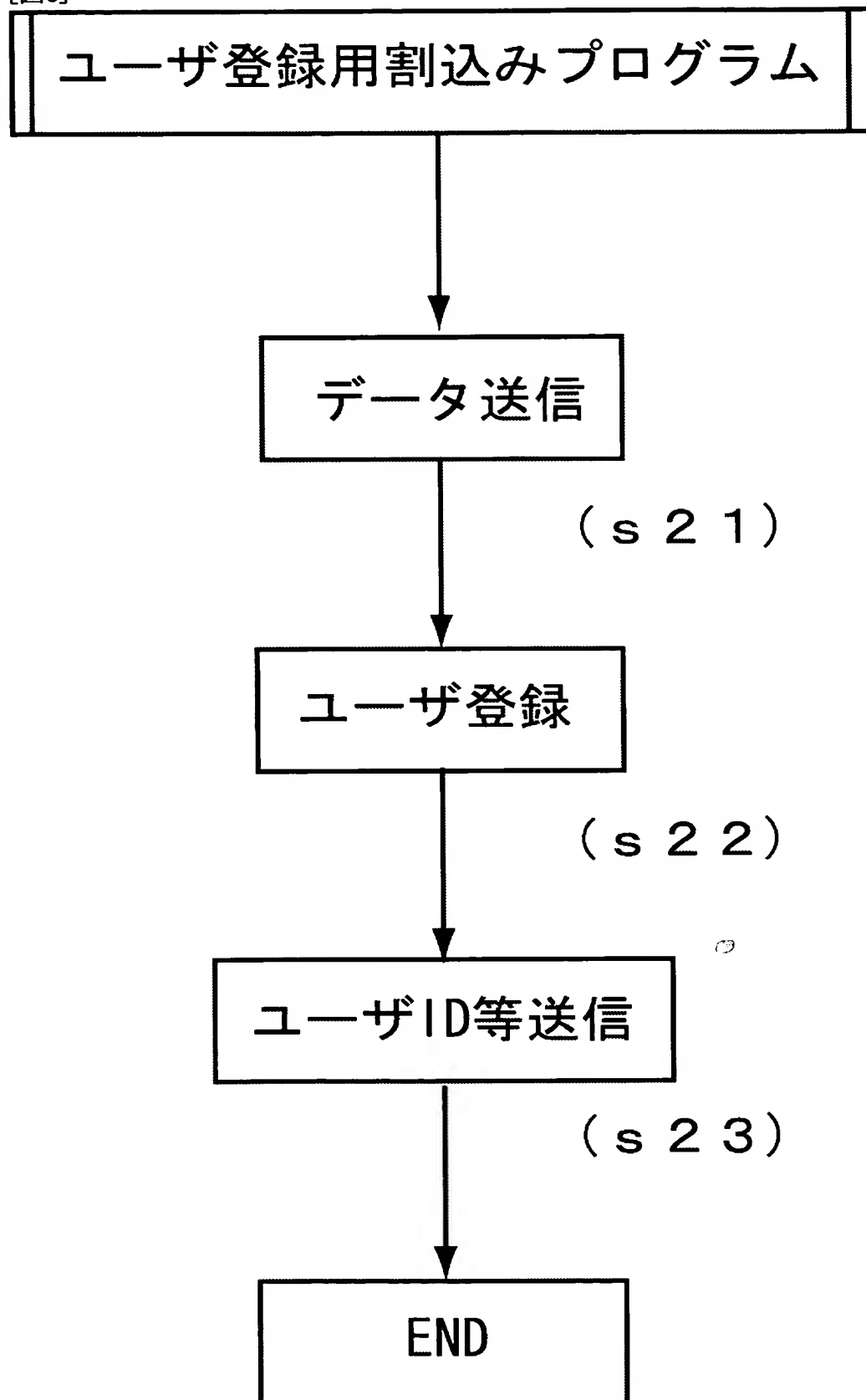




[図7]

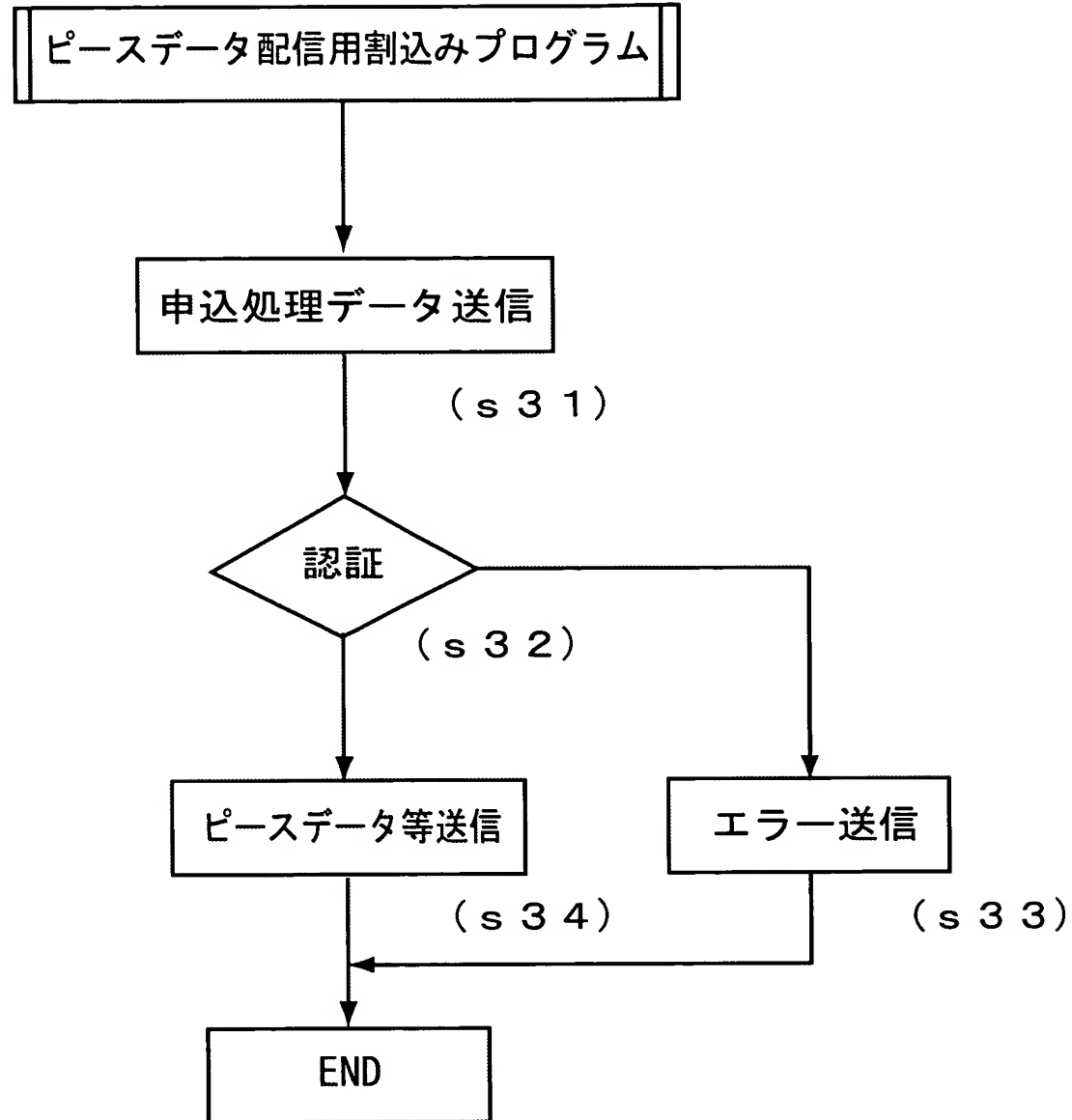


[図8]



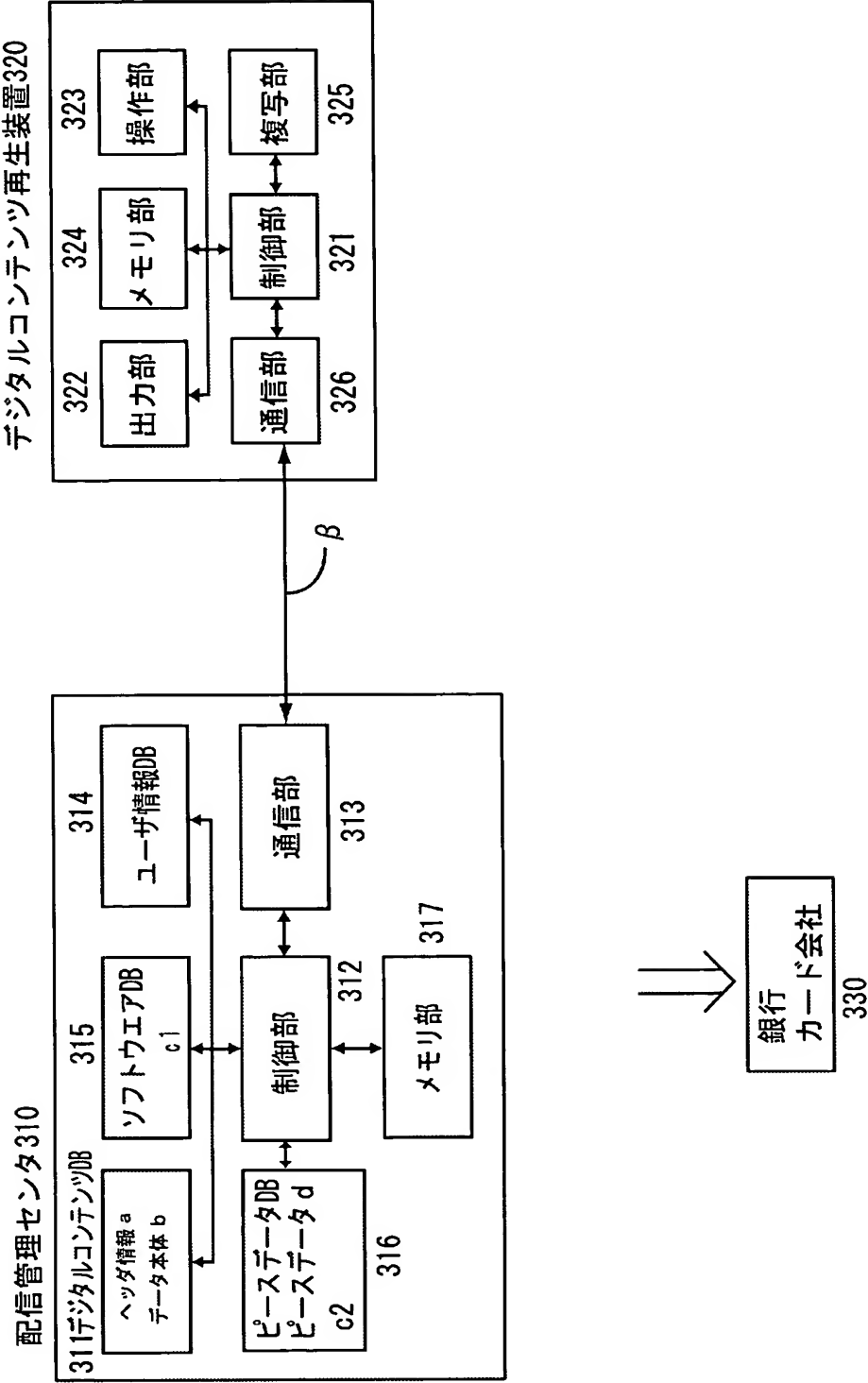


[図9]

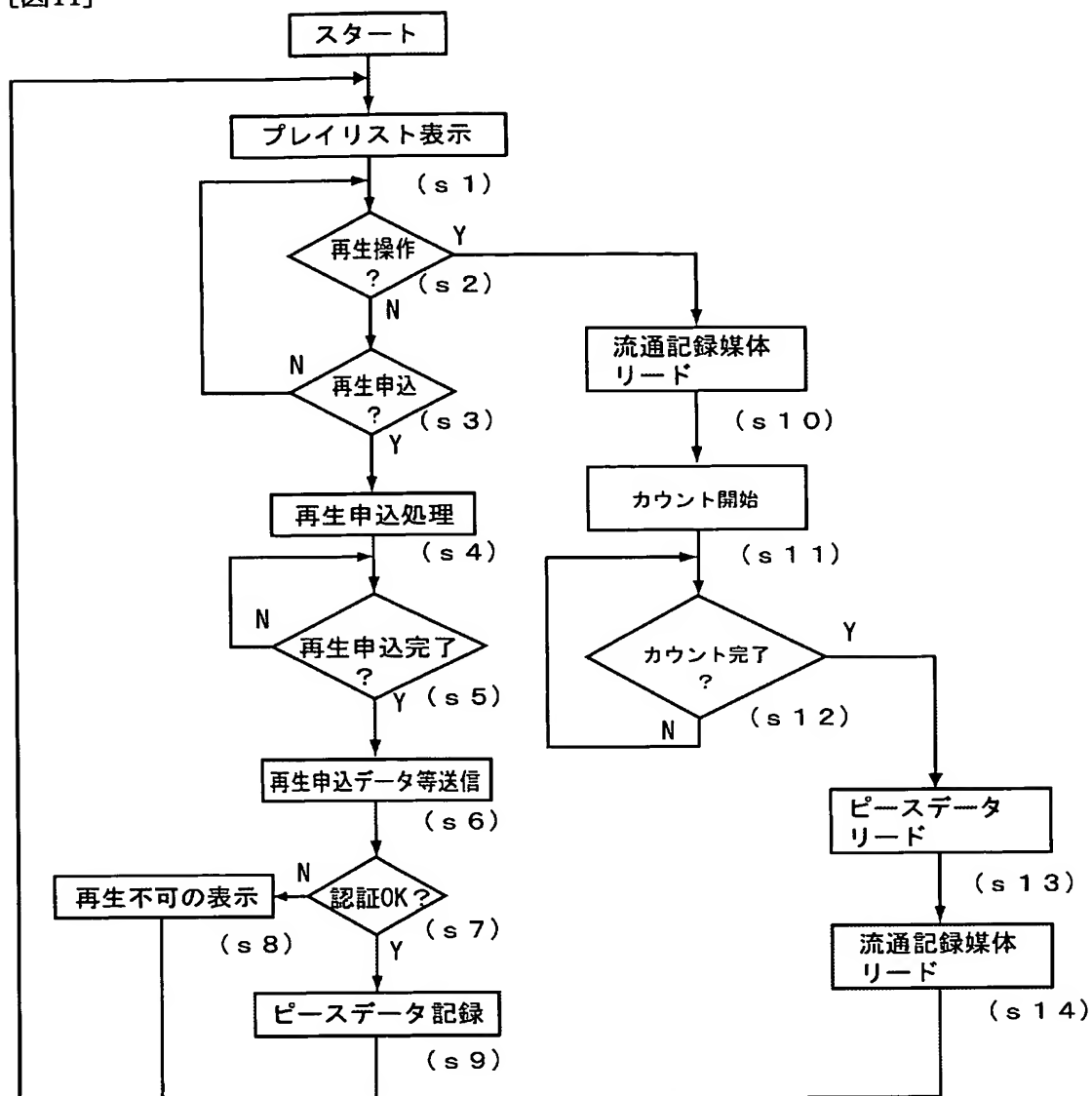


300

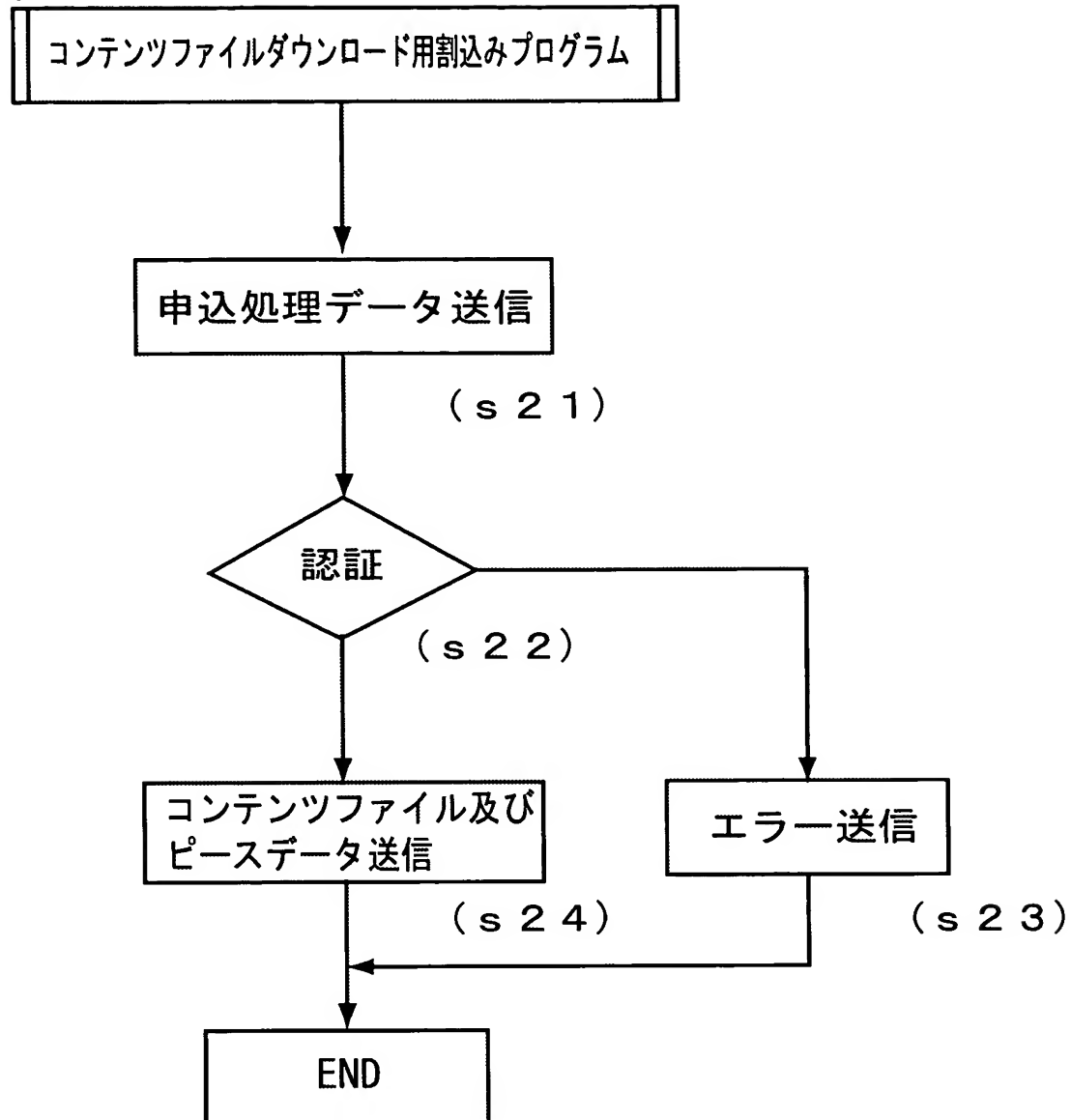
[図10]



[図11]

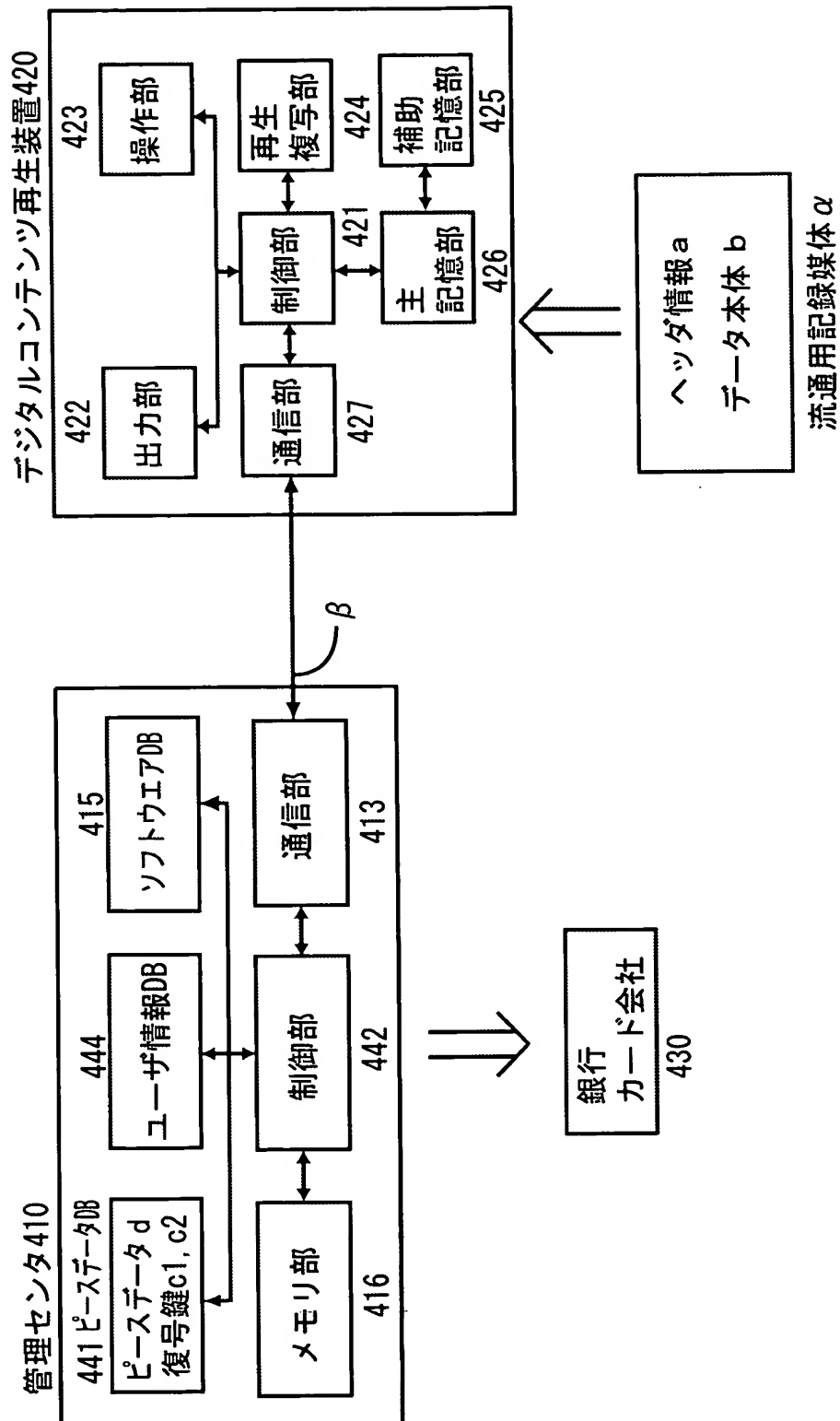


[図12]

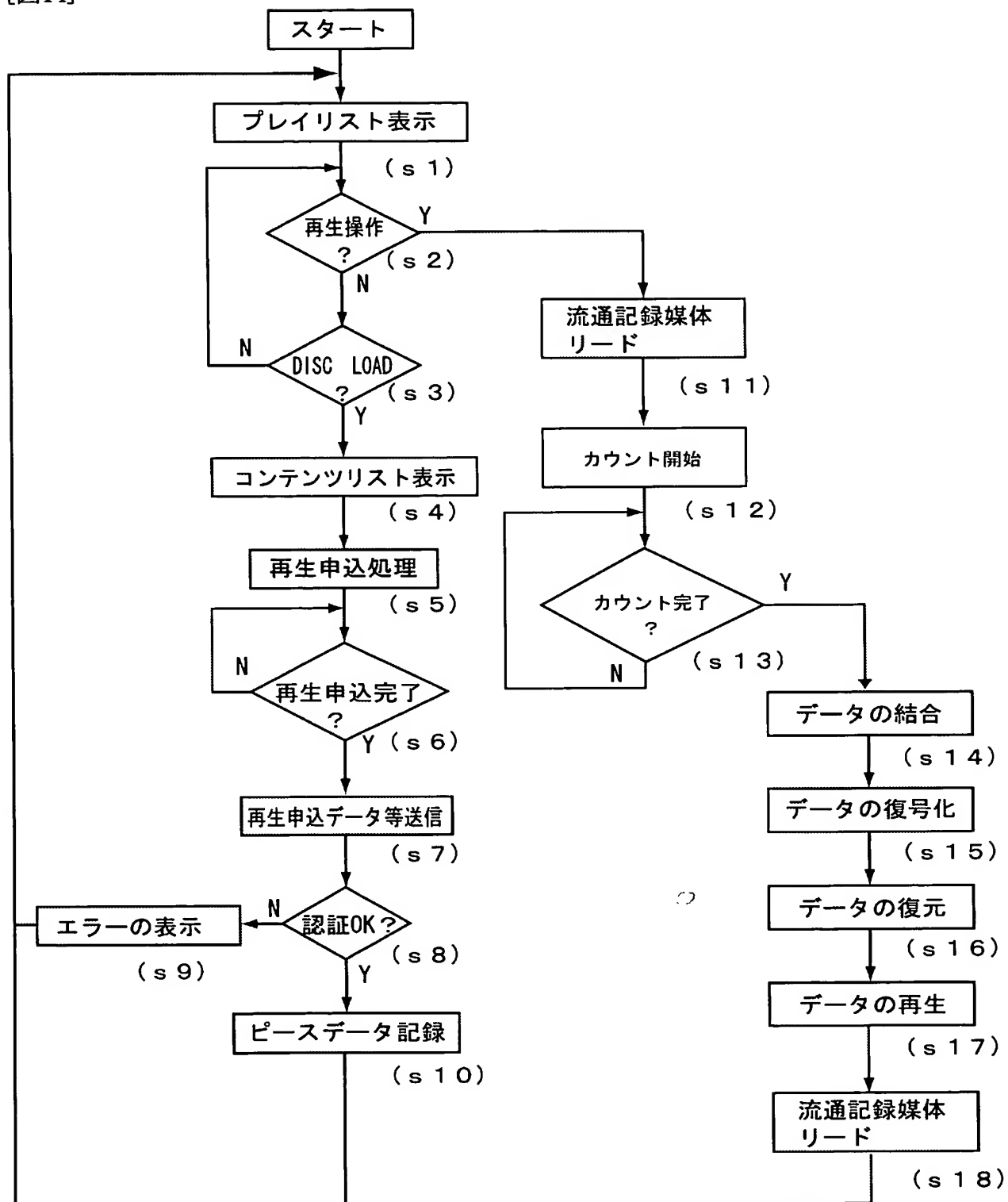


[図13]

400

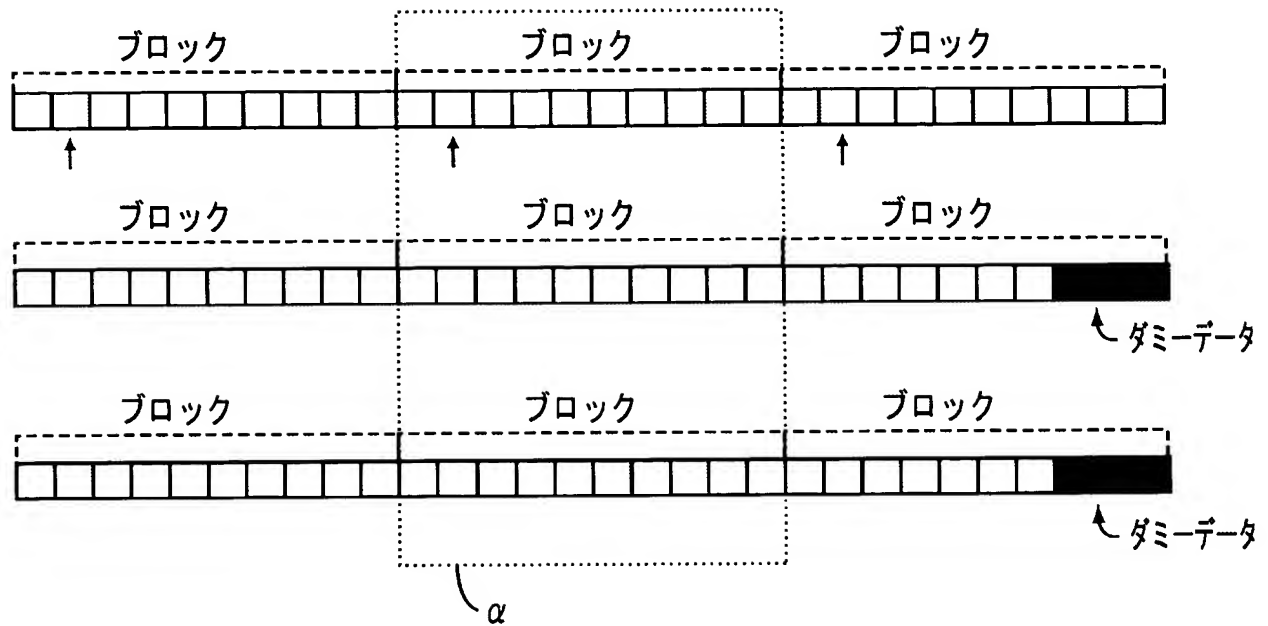


[図14]



[図15]

(a)

b データ本体

(b)

暗号化 .....7503194628.....

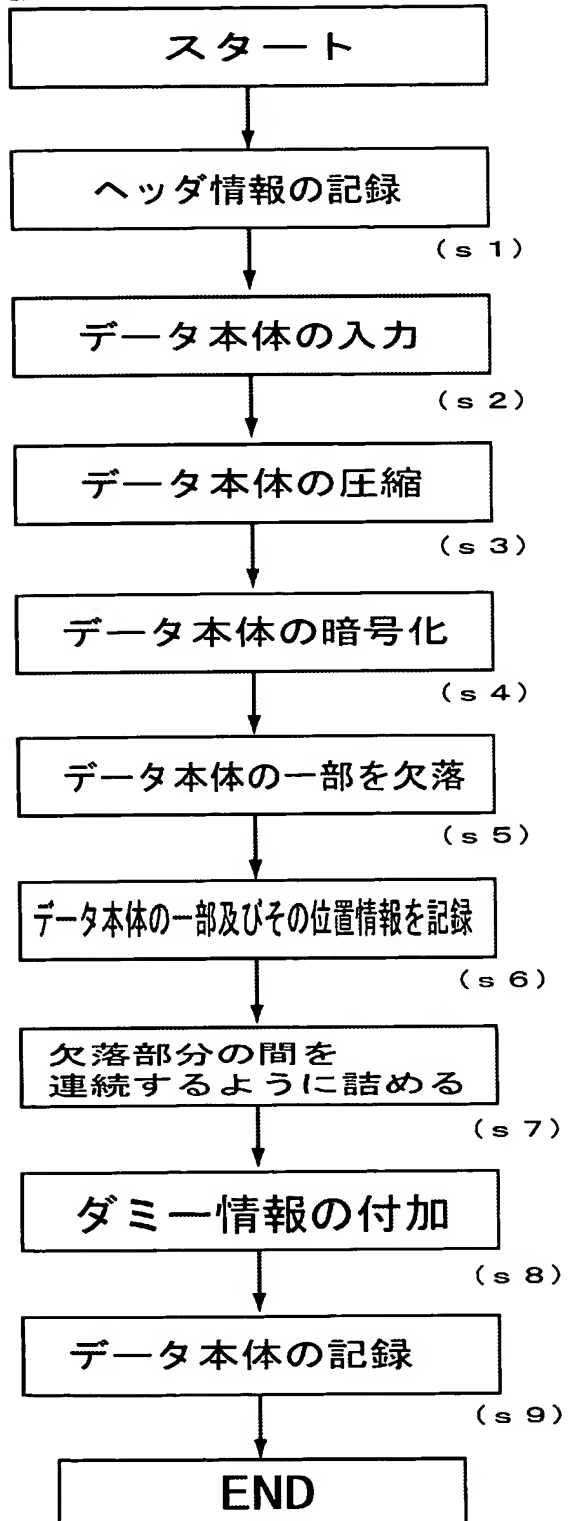
↓

一部を欠落 .....7□03194628.....

↓

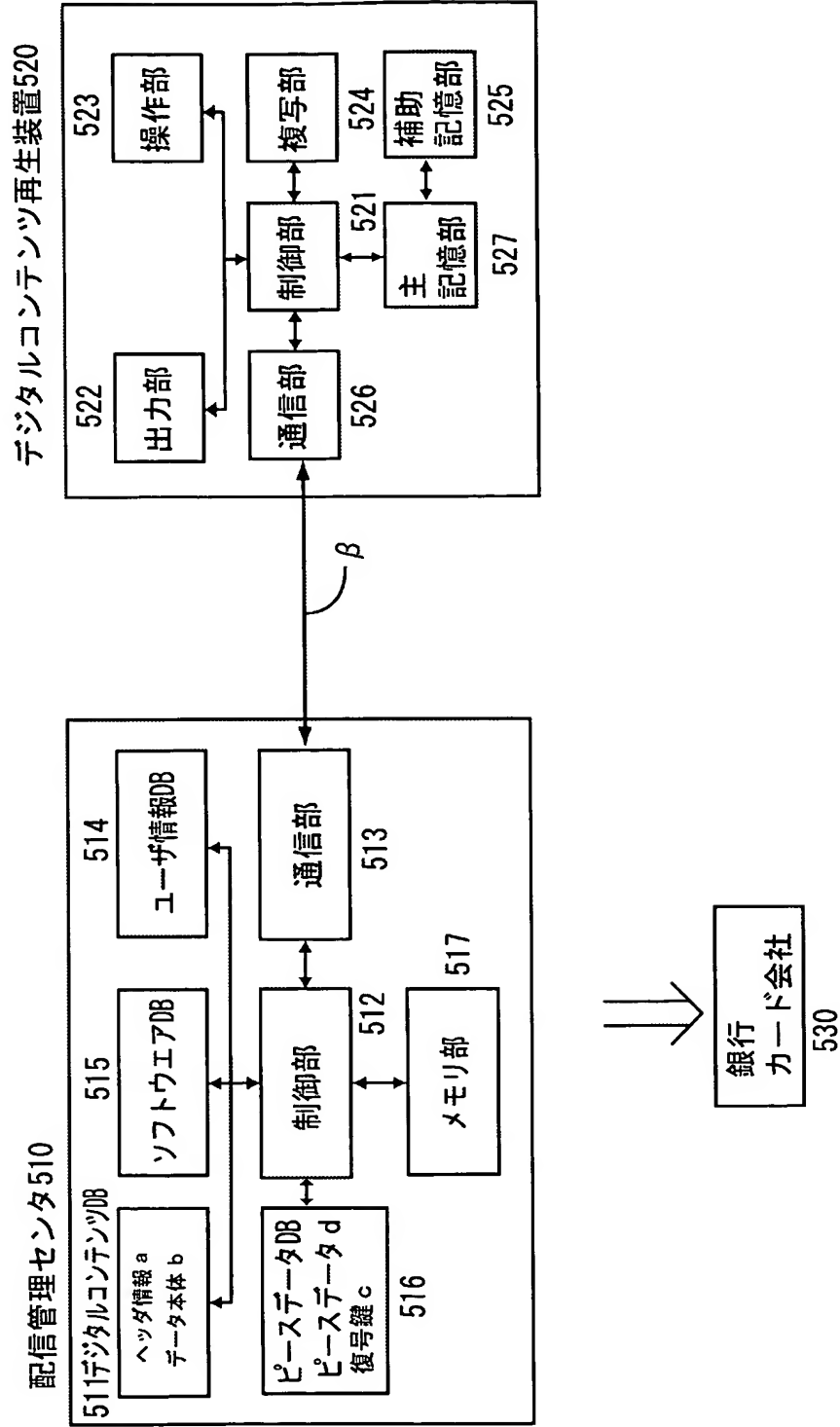
欠落部分  
の間を詰める .....7031946286.....

[図16]

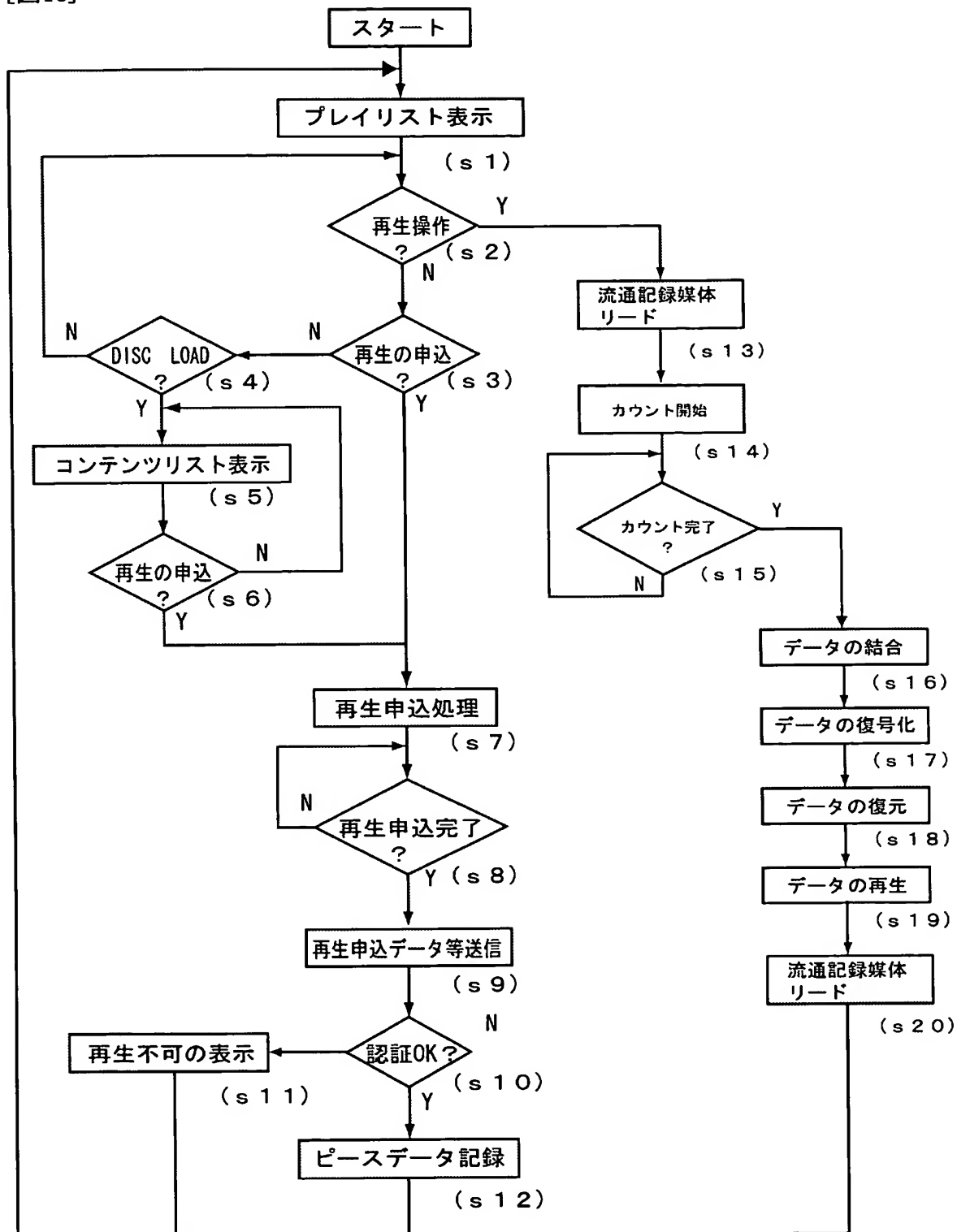




[図17]



[図18]



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/013331

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L9/08, H04L9/28, G06F17/60, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> H04L9/08, H04L9/28, G06F17/60, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-115162 A (Kabushiki Kaisha Kodo Ido Tsushin Security Gijutsu Kenkyusho), 21 April, 2000 (21.04.00), Full text; all drawings (Family: none)	1-13
Y	JP 5-316079 A (Sony Corp.), 26 November, 1993 (26.11.93), Par. Nos. [0020] to [0023]; Figs. 2 to 4 (Family: none)	1-13

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
03 December, 2004 (03.12.04)

Date of mailing of the international search report  
21 December, 2004 (21.12.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/013331

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 9-8797 A (Nippon Telegraph And Telephone Corp.), 10 January, 1997 (10.01.97), Par. Nos. [0025], [0026], [0029], [0032]; Figs. 1 to 3 (Family: none)	3
Y	JP 4-200125 A (Matsushita Electric Industrial Co., Ltd.), 21 July, 1992 (21.07.92), Page 2, lower right column, line 18 to page 3, upper left column, line 3; Figs. 4, 6 (Family: none)	10,11

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/08, H04L9/28, G06F17/60, G06F12/14

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/08, H04L9/28, G06F17/60, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2000-115162 A (株式会社高度移動通信セキュ リティ技術研究所) 2000.04.21 全文, 全図 (ファミリーなし)	1-13
Y	JP 5-316079 A (ソニー株式会社) 1993.11.26 第【0020】-【0023】段落, 図2-4 (ファミリーなし)	1-13

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に関する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

03.12.2004

国際調査報告の発送日

21.12.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 9-8797 A (日本電信電話株式会社) 1997. 01. 10 第【0025】 , 【0026】 段落, 第【0029】 段落, 第【0032】 段落, 図1-3 (ファミリーなし)	3
Y	JP 4-200125 A (松下電器産業株式会社) 1992. 07. 21 第2頁右下欄第18行-第3頁左上欄第3行, 図4, 6 (ファミリーなし)	10, 11